CS Exit Ethiopia

Questions & Worked Answers

Computer Science Exit Examination

274 complete questions and 1 source variants

1 selected course | 18 November 2026

Selected courses

01. Data Communication and Computer Networking

https://csexitethiopia.com

abelasnake2003@gmail.com | Telegram: @Abechu7

Course contents

Each course begins on a new page. PDF bookmarks provide question, study-note section and revision-topic navigation.

Data Communication and Computer Networking 3

Reading the answers

Every question includes its answer, explanation, choice-by-choice contrasts and available evidence. Primary note proof quotes the study notes. Related reading and module passages are labelled separately; a module reference is not presented as primary note proof.

Data Communication and Computer Networking

Questions & Worked Answers

274 questions + 1 source variants

Question 1 | Q00016

Which term describes combining multiple analogue or digital input signals for transmission over one shared medium?

A. Point-to-point

B. Broadcasting

C. Synchronization

D. Multiplexing

Hint

Compare the signal mechanism, medium properties or transmission direction against the definitions and stated physical assumptions.

Answer D: Multiplexing

Multiplexing combines separate input streams so they can share a transmission link. The receiver uses demultiplexing to separate them again. This operation concerns sharing link capacity, whereas broadcasting concerns the recipients of a message. Point-to-point describes the endpoints of a link, and synchronization coordinates timing. The option supplies the required operation while preserving those distinctions.

Why each choice is right or wrong

A - Incorrect: Point-to-point joins two endpoints and does not mean combining input signals onto a shared link.

B - Incorrect: Broadcast sends a message to all destinations in scope rather than combining multiple input streams.

C - Incorrect: Synchronization coordinates timing; it is not the multiplexing operation defined by the stem.

D - Correct: Multiplexing combines multiple streams for a shared link and is precisely the operation described.

Primary note proof

Study-note section NET32

> Multiplexing combines multiple input streams onto a shared link; demultiplexing separates them at the receiver. It differs from broadcasting one message to many destinations. FDM

assigns distinct frequency bands with suitable guard spacing; WDM assigns different optical wavelengths. TDM allocates time slots: synchronous TDM reserves recurrent slots even if an input is idle, while statistical TDM allocates according to demand and needs identification.

Study-note section NET08

Physical topology describes link layout; logical topology describes communication/access relationships. Point-to-point links join two endpoints; multipoint links share a medium. A full mesh consists of point-to-point links.

Study-note section NET06

Simplex is one way, half duplex alternates directions, and full duplex permits simultaneous sending/receiving. A walkie-talkie is half duplex; a telephone conversation uses full duplex. Serial sends sequential bits; parallel uses multiple conductors and may suffer skew. Character-oriented asynchronous serial adds start/stop bits; synchronous framing uses ongoing clock recovery. Neither is synonymous with browser asynchronous requests.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 20 | lines 37-42

MULTIPLEXING
Whenever the bandwidth of a medium linking two devices is greater than the bandwidth needs of the devices, the link can be shared. Multiplexing is the set of techniques that allows the simultaneous transmission of multiple signals across a single data link.

Data Communication and Computer Networking module | PDF page 11 | lines 34-51

NETWORK TOPOLOGY
A network topology is a description of the layout of the region or area covered by that network.
There are two types of connections. They are: point-to-point and multi-point.
Point-to-point connections provide a direct link between two devices.
Multi-point connections provide a link between three or more devices on a network.
There are seven basic topologies in the study of network topology:
• Point-to-point topology,
• Bus (point-to-multipoint) topology,
• Ring topology,
• Star topology,
• Hybrid topology,
• Mesh topology and,
• Tree topology.

Data Communication and Computer Networking module | PDF page 17 | lines 54-59

> ICMP- Internet Control Message Protocol: It is a signaling mechanism used to inform the sender about datagram problemsthat occur during transit. It is used by intermediate devices.
> IGMP- Internet Group Message Protocol: It is a mechanism that allows sending the same message to a group of recipients.

Question sources

MOE Computer Science Exit Exam · 2016 · Question 16

Question 2 | Q00036

A traditional phone call is an example of

A. Packet switching

B. Multiplexing

C. Broadcasting

D. Circuit switching

Hint

Use the cited note definitions to identify the requested function or scope, then check each alternative against that same rule.

Answer D: Circuit switching

A traditional circuit telephone call exemplifies establishment, continuous use of a dedicated path, and release. This applies to the traditional circuit service assumed by the stem, rather than all modern telephone implementations. Evidence: PDF 20, 20, 20.

Why each choice is right or wrong

A - Incorrect: Packets are discrete rather than the dedicated circuit described (PDF 20, 20, 20.)

B - Incorrect: Multiplexing shares a link and may underlie telephony but does not name its switching service (PDF 20, 20, 20.)

C - Incorrect: Broadcasting does not establish a dedicated pairwise call (PDF 20, 20, 20.)

D - Correct: Dedicated establishment, transfer and disconnect match the call (PDF 20, 20, 20.)

Primary note proof

Study-note section NET31

> Circuit switching sets up a path with reserved resources, transfers data, then releases it. Predictable allocated bandwidth trades against setup/blocking and wasted reservation during silence. A traditional telephone call is the standard example. Packet switching divides data into packets that share links statistically; queueing can add variable delay and loss. This does not

make modern voice-over-packet impossible: buffering, scheduling and capacity planning manage it.

Study-note section NET32

Multiplexing combines multiple input streams onto a shared link; demultiplexing separates them at the receiver. It differs from broadcasting one message to many destinations. FDM assigns distinct frequency bands with suitable guard spacing; WDM assigns different optical wavelengths. TDM allocates time slots: synchronous TDM reserves recurrent slots even if an input is idle, while statistical TDM allocates according to demand and needs identification.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 20 | lines 12-26

Circuit Switching: In circuit switching, two communicating stations are connected by a dedicated communication path which consists of intermediate nodes in the network and the links that connect these nodes.
It involved the following three distinct steps
• Circuit Establishment: To establish an end-to-end connection before any transfer of data.
• Data transfer: Transfer data is from the source to the destination. The data may be analog or digital, depending on the nature of the network. The connection is generally full-duplex.
• Circuit disconnect: Terminate connection at the end of data transfer. Signals must be propagated to deallocate the dedicated resources.

Data Communication and Computer Networking module | PDF page 20 | lines 27-36

Message Switching:
Packet Switching: Packet switching was designed to address the shortcomings of circuit switching in dealing with data communication. Unlike circuit switching where communication is continuous along a dedicated circuit, in packet switching, communication is discrete in form of packets.
The three switching modes to choose from are:
• Cut-through
• Store-and-forward
• Fragment-free

Data Communication and Computer Networking module | PDF page 20 | lines 37-42

MULTIPLEXING
Whenever the bandwidth of a medium linking two devices is greater than the bandwidth needs of the devices, the link can be shared. Multiplexing is the set of techniques that allows the

simultaneous transmission of multiple signals across a single data link.

Question sources

MOE Computer Science Exit Exam · 2016 · Question 36

Question 3 | Q00050

Assume you are searching for information and typed the domain name: www.mysearchexample.com on your browser, having an IP address 192.108.110.1. Since internet communication is based on an IP address, the domain name has to be translated to its corresponding IP address. Which of the following is responsible for the translation?

A. DNS

B. SMTP

C. FTP

D. DHCP

Hint

Separate address width, syntax, reserved scope and the supplied prefix or historical classful convention.

Answer A: DNS

The needed operation is name resolution. The module identifies DNS as Domain Name Service and contrasts external DNS naming with locally stored host addresses; together these support the name-to-address lookup. Evidence: PDF 18, 65, 18.

Why each choice is right or wrong

A - Correct: DNS is the named external naming service (PDF 18, 65, 18.)

B - Incorrect: SMTP is electronic mail, not name lookup (PDF 18, 65, 18.)

C - Incorrect: FTP is file transfer, not name lookup (PDF 18, 65, 18.)

D - Incorrect: Page28 explicitly expands DHCP as Dynamic Host Configuration Protocol, separately from DNS (Domain Name Service). The external naming service discussed on page65 is DNS, the operation requested, rather than the separately named host-configuration protocol. The expansion alone is not a full account of DHCP operation.

Primary note proof

Study-note section NET20

DNS resolves names to records, including IPv4 A and IPv6 AAAA addresses; it can use UDP or TCP port 53. DHCP dynamically leases IPv4 settings, commonly address, mask, gateway and DNS server. Its basic exchange is discover, offer, request, acknowledge. IP itself does not assign addresses.

Study-note section NET21

HTTP defines web request/response semantics; it is stateless, and a message body may be absent. HTTPS adds TLS protection. FTP transfers files using control and separate data connections; it is not the same protocol as SFTP. SMTP submits and relays mail; POP3 retrieves messages and IMAP accesses/synchronizes server mailboxes. Saying SMTP handles both sending and end-user mailbox retrieval is inaccurate.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 18 | lines 27-32

Application Layer
The Application Layer is a combination of Session,
Presentation & Application Layers of OSI models and defines
high level protocols like File Transfer (FTP), Electronic Mail
(SMTP), Virtual Terminal (TELNET), Domain Name Service
(DNS), etc.

Data Communication and Computer Networking module | PDF page 65 | lines 31-38

/etc/hosts
The /etc/hosts file always contains the localhost IP
address, 127.0.0.1, which is
usedfor interprocess communication.
Never remove this line! Sometimes contains
addresses of additional hosts, whichcan be contacted
without using an external naming service such as
DNS (the Domain Name Server).

Data Communication and Computer Networking module | PDF page 18 | lines 9-21

TCP - Transmission Control Protocol: TCP is a reliable
connection-oriented, reliable protocol. i.e. a connection is
established between the sender and receiver before the data can
be transmitted. It divides the data it receives from the upper
layer into segments and tags a sequence number to each
segment which is used at the receiving end for reordering of
data.
UDP - User Datagram Protocol: UDP is a simple protocol
used for process to process transmission. It is an unreliable,
connectionless protocol for applications that do not require flow
control or error control. It simply adds port address, checksum
and length information to the data it receives from the upper
layer.

Data Communication and Computer Networking module | PDF page 28 | lines 37-45

The Process/Application Layer Protocols
• Telnet

- File Transfer Protocol (FTP)
- Network File System (NFS).
- Simple Mail Transfer Protocol (SMTP
- POP3 is used to receive mail.
- Simple Network Management Protocol (SNMP)
- Domain Name Service (DNS)
- Dynamic Host Configuration Protocol (DHCP)

Question sources

MOE Computer Science Exit Exam · 2016 · Question 50

Question 4 | Q00061

Which one of the following is not correct about networking models?

A. TCP/IP model is a protocol model

B. A reference model has no implementation specification

C. A network designer can use either of TCP/IP or OSL, or both

D. Open system interconnection (OSI) is a protocol model

Hint

Use the cited note definitions to identify the requested function or scope, then check each alternative against that same rule.

Answer D: OSI is a reference model, not itself an implemented protocol suite

NET03 distinguishes an abstract reference model from an implemented protocol suite. D incorrectly calls OSI a protocol model in that distinction. TCP/IP supplies the implemented suite, and designers can use models as architectural guides. B is valid when understood as the model itself not providing executable implementation details, rather than denying all interface descriptions.

Why each choice is right or wrong

A - Incorrect: TCP/IP describes an implemented protocol suite, consistent with calling it a protocol model.

B - Incorrect: A reference model divides responsibilities/interfaces without itself being executable implementation software.

C - Incorrect: Models can guide network design; using one or both perspectives is compatible with their reference purpose.

D - Correct: OSI is the reference model in the stated contrast, not itself the implemented TCP/IP-style protocol suite.

Primary note proof

Study-note section NET03

A reference model divides responsibilities and interfaces; it is not itself executable networking software. OSI is a seven-layer reference model; TCP/IP describes an implemented protocol suite, usually taught with four layers. A five-layer teaching model separates physical and link functions. State the model before counting layers.

Study-note section NET19

The four-layer TCP/IP model folds OSI layers 5-7 into application, retains transport, calls layer 3 Internet, and combines link/physical as network access. A model is a guide to functions, not a guarantee that every application gets a reliable network. Distinguish end-to-end application service from its underlying process-to-process transport.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 14 | lines 12-29

The Open Systems Interconnection (OSI) Model was
developed by International Organization for Standardization
(ISO). ISO is the organization, OSI is the model
It was developed to allow systems with different platforms
(Hardware & software) to communicate with each other.
Now, it is a network model that defines the protocols for
network communications.
It is a hierarchical model that groups its processes into seven
(7) layers. (Top to Bottom)
1. Application Layer
2. Presentation Layer
3. Session Layer
4. Transport Layer
5. Network Layer
6. Data Link Layer
7. Physical Layer
Each layer has specific functions to perform and has to co-
operate with the layers above and below it.

Data Communication and Computer Networking module | PDF page 16 | lines 50-59

After understanding the concept of layered task and the OSI
model, we introduce the TCP/IP model. This model is
currently being used on our systems. TCP/IP model is a
collection of protocols often called a protocol suite. It offers a
rich variety of protocols.
It is a hierarchical model; it existed even before the OSI model
was developed. Originally had four layers (bottom to top):
1. Host to Network Layer
2. Internet Layer
3. Transport Layer

Data Communication and Computer Networking module | PDF page 25 | lines 17-27

TCP/IP is a hierarchical protocol made up of interactive modules, each of which provides a specific functionality; however, the modules are not necessarily interdependent. Whereas the OSI model specifies which functions belong to each of its layers, the layers of TCP/IP suite contain relatively independent protocols that can be mixed and matched depending on the needs of the system. The term hierarchical means that each upper-level protocol is supported by one or more lower-level protocols.

Question sources

MOE Computer Science Exit Exam · 2016 · Question 61

Question 5 | Q00063

Which statement about IPv4 is incorrect?

A. It uses 128-bit addresses.

B. Its finite address space has faced allocation scarcity.

C. Private addressing with NAT can conserve public IPv4 addresses.

D. It uses 32-bit addresses.

Hint

Separate address width, syntax, reserved scope and the supplied prefix or historical classful convention.

Answer A: It uses 128-bit addresses.

IPv4 addresses contain 32 bits, whereas IPv6 uses a much larger address space. IPv4 allocation scarcity motivates conservation through private addressing and NAT. These are address-space properties, not a claim that every IPv4 router is intrinsically slow or memory-intensive. The incorrect statement assigns a 128-bit address width to IPv4.

Why each choice is right or wrong

A - Correct: IPv4 addresses are 32 bits, so the claimed 128-bit width is incorrect.

B - Incorrect: Finite IPv4 address allocation has faced scarcity; this statement is true.

C - Incorrect: Private addressing with NAT conserves public IPv4 addresses; this statement is true.

D - Incorrect: The stated 32-bit IPv4 address width is correct.

Primary note proof

Study-note section NET16

IP supplies connectionless best-effort packet delivery, not end-to-end ordering or retransmission. IPv4 addresses are 32 bits. Its minimum header is 20 bytes and can grow to 60 bytes; it is not a 32-bit header. IHL counts 32-bit words; total length includes header and payload. TTL limits lifetime across routers; the protocol field identifies TCP, UDP or another upper-layer protocol.

Study-note section NET-S03

The finite IPv4 address space has faced allocation scarcity. Private addressing with NAT conserves public IPv4 addresses, while IPv6 provides a much larger address space.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 18 | lines 45-54

IP addresses: IP address uniquely identifies a device on the Internet. Every host and router on the Internet has an IP address, which encodes its network number and host number.
• The combination is unique: in principle, no two machines on the Internet have the same IP address.
• An IPv4 address is 32 bits long
• They are used in the Source address and Destination address fields of IP packets.
• An IP address does not refer to a host but it refers to a network interface.

Data Communication and Computer Networking module | PDF page 19 | lines 45-49

NAT (Network Address Translation): The scarcity of network addresses in IPv4 led to the development of IPv6. Due to this, we need to use private IP address inside the organization and translate it to public IP address using NAT.

Question sources

MOE Computer Science Exit Exam · 2016 · Question 63

Question 6 | Q00073

Which item is not a transmission impairment?

A. Synchronization

B. Crosstalk

C. Impulse noise

D. Distortion

Hint

Compare the signal mechanism, medium properties or transmission direction against the definitions and stated physical assumptions.

Answer A: Synchronization

Distortion changes the signal's shape, while crosstalk and impulse noise add unwanted disturbances. Crosstalk couples energy from a nearby channel; impulse noise is a brief disturbance. Synchronization instead aligns timing so the receiver can interpret transmitted symbols. Losing synchronization can cause errors, but synchronization itself is a desirable coordination process rather than one of these signal impairments.

Why each choice is right or wrong

A - Correct: Synchronization aligns timing and is not itself an impairment.

B - Incorrect: Crosstalk is unwanted coupling from nearby channels, a noise impairment.

C - Incorrect: Impulse noise is a short unwanted disturbance, a noise impairment.

D - Incorrect: Distortion changes the signal shape and is a transmission impairment.

Primary note proof

Study-note section NET06

> Attenuation reduces signal strength. Distortion changes shape, often because frequencies have different delays. Noise adds unwanted energy: thermal noise comes from random thermal motion, crosstalk leaks from nearby channels, and impulse noise is a short disturbance. Amplifiers amplify noise too; digital repeaters regenerate decisions but cannot reconstruct every corrupted bit.

Study-note section NET06

> Simplex is one way, half duplex alternates directions, and full duplex permits simultaneous sending/receiving. A walkie-talkie is half duplex; a telephone conversation uses full duplex. Serial sends sequential bits; parallel uses multiple conductors and may suffer skew. Character-oriented asynchronous serial adds start/stop bits; synchronous framing uses ongoing clock recovery. Neither is synonymous with browser asynchronous requests.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 10 | lines 18-35

> receiver.There are three causes of impairment:
> • Attenuation
> • Distortion
> • Noise
> Attenuation
> Attenuation results in loss of energy due to distance.
> Whena signal travels through a medium, it loses some
> of its energy in overcoming the resistance of the

medium. The electrical energy in the signal may convert to heat. To compensate for this loss, amplifiers are used to amplify thesignal.
Distortion
Distortion changes the shape of the signal.
Noise
Noise is any unwanted signal that is mixed or combined with the original signal during transmission. Due to noise the original signal is altered and signal received is not sameas the one sent.

Data Communication and Computer Networking module | PDF page 14 | lines 50-55

• Synchronization of bits: To interpret correct and accurate data the sender and receiver have to maintain the same bit rate and also have synchronized clocks.
• Line configuration: The physical layer defines the nature of the connection .i.e. a point to point link, or a multi-point link.

Question sources

MOE Computer Science Exit Exam · 2016 · Question 73

Question 7 | Q00086

_____ is a probabilistic algorithm where a data packet is sent by the router to any one of its neighbors randomly.

A. Adaptive routing algorithm

B. Flooding routing algorithm

C. Random walks routing algorithm

D. Distributed routing algorithm

Hint

Compare signal repetition, frame forwarding, packet routing and policy enforcement using the stated device or traffic assumptions.

Answer C: Random-walk routing

NET30 defines a random walk by probabilistically choosing a neighbor, exactly the forwarding behavior in the stem. Flooding instead replicates packets. Adaptive and distributed describe broader properties of routing algorithms; neither alone specifies random single-neighbor selection.

Why each choice is right or wrong

A - Incorrect: Adaptive routing responds to network conditions; adaptation alone does not mean choosing a random neighbor.

B - Incorrect: Flooding sends copies on multiple eligible links rather than selecting just one neighbor randomly.

C - Correct: Random walk selects the next neighbor probabilistically, matching the stated packet-forwarding procedure.

D - Incorrect: Distributed routing spreads computation among routers; it does not specify the random choice described.

Primary note proof

Study-note section NET30

> Flooding sends copies on eligible outgoing links with duplicate/lifetime controls; random walk picks a neighbor probabilistically. Unicast targets one destination, broadcast all in a scope, multicast a subscribed group and anycast one member sharing an address, normally nearest under routing metrics. Multi-destination packets can list multiple targets; this is not necessarily identical to broadcast. Group multicast trees use mechanisms such as reverse-path checks; Ethernet spanning tree is a different layer-2 mechanism.

Study-note section NET-S01

> Adaptive or dynamic routing changes routes in response to updated network information; nonadaptive or static routing uses configured choices. Distributed routing means routers perform computations using exchanged information instead of requiring one central route computation. These properties do not imply random next-hop selection: the path-selection rule is a separate classification.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 19 | lines 52-64

> ROUTING AND ROUTING PROTOCOLS
> Routing is the act of moving information across an internetwork from a source to a destination. At the heart of such protocol is the routing algorithm that determines the path for a packet.
> • Routing requires a host or a router to have a routingtable which is constructed by the routing algorithm.
> • There are wo kinds of routing algorithms (routing tables): nonadaptive (static) and adaptive (dynamic)
> • And two kinds of protocols
> o Interior routing protocols
> o Exterior routing protocols

Question sources

MOE Computer Science Exit Exam · 2016 · Question 86

Question 8 | Q00087

Which network address translation protocol solves the task of address resolution using port number?

A. Network Address Translation

B. Port Address Translation

C. Dynamic Address Translation

D. Static address translation

Hint

Convert the mask to a prefix, separate network and host bits, and apply the relevant subnet-count or usable-host rule.

Answer B: Port Address Translation (PAT/NAPT)

The wording loosely calls translation “address resolution,” but its decisive qualifier is use of port numbers. NET29 identifies PAT/NAPT as translation of address-plus-port combinations, allowing shared public addresses. This is not hardware-address resolution by ARP, and ordinary static or pooled dynamic address mappings do not themselves describe port multiplexing.

Why each choice is right or wrong

A - Incorrect: NAT is the broad translation family; this option does not identify the port-based form specifically.

B - Correct: PAT translates address-and-port combinations, distinguishing simultaneous clients that share an external address.

C - Incorrect: Dynamic NAT allocates address mappings from a pool, without necessarily multiplexing transport ports.

D - Incorrect: Static NAT fixes an address mapping; port-based sharing is the separate PAT mechanism.

Primary note proof

Study-note section NET29

> Static NAT gives a fixed address mapping; dynamic NAT allocates mappings from a pool. PAT/NAPT maps address-plus-port combinations so multiple private clients share a public address. It is translation, not ARP resolution and not encryption. Return traffic must match the translation state or a configured inbound mapping.

Study-note section NET20

> ARP resolves an on-link IPv4 next hop to a link address, using a broadcast request and normally unicast reply. For an off-subnet target, ARP resolves the gateway, not the remote target’s MAC. It

bridges the network/link addressing boundary and is often classified at the link layer; calling ARP simply a network protocol uses a loose textbook convention. RARP reverses hardware-to-IP lookup; BOOTP/DHCP support boot configuration. ICMP reports errors and diagnostics; IGMP manages IPv4 multicast membership. These are separate companion protocols, not four pieces whose combination is IP.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 19 | lines 45-49

NAT (Network Address Translation): The scarcity of network addresses in IPv4 led to the development of IPv6. Due to this, we need to use private IP address inside the organization and translate it to public IP address using NAT.

Data Communication and Computer Networking module | PDF page 48 | lines 29-40

Network Address Translation (NAT)
NAT translates the IP addresses of computers in a local network to a single IP address. This address is often used by the router that connects the computers to the Internet. The router can be connected to a DSL modem, cable modem, T1 line, or even a dial-up modem. When other computers on the Internet attempt to access computers within the local network, they only see the IP address of the router. This adds an extra level of security, since the router can be configured as a firewall, only allowing authorized systems to access the computers within the network.

Data Communication and Computer Networking module | PDF page 28 | lines 2-14

TCP and UDP must use port numbers to communicate with the upper layers, because they‘re what keep track of different conversations crossing the network simultaneously. These port numbers identify the source and destination application or process in the TCP segment. There are 216 = 65,536 ports available.
Well-known ports: The port numbers range from 0 to 1,023.
Registered ports: The port numbers range from 1,024 to 49,151. Registered ports are used by applications or services that need to have consistent port assignments.
Dynamic or private ports: The port numbers range from 49,152 to 65,535.

Question sources

MOE Computer Science Exit Exam · 2016 · Question 87

Question 9 | Q00088

Which protocol resolves a known on-link IPv4 next-hop address to its link-layer hardware address?

A. Address Resolution Protocol (ARP)

B. Reverse Address Resolution Protocol (RARP)

C. Bootstrap Protocol (BOOTP)

D. Internet Control Message Protocol (ICMP)

Hint

Convert the mask to a prefix, separate network and host bits, and apply the relevant subnet-count or usable-host rule.

Answer A: Address Resolution Protocol (ARP)

ARP resolves an on-link IPv4 next hop to a link address, normally by broadcasting a request and receiving a reply. For an off-subnet destination, the next hop is usually the gateway rather than the remote destination itself. RARP reverses hardware-to-IP lookup; BOOTP supplies boot configuration, and ICMP carries network diagnostics. These distinct functions do not replace ARP's local IPv4-to-link resolution.

Why each choice is right or wrong

A - Correct: ARP resolves the known local IPv4 next hop to its link address.

B - Incorrect: RARP performs the reverse hardware-to-IP lookup.

C - Incorrect: BOOTP supplies boot configuration rather than resolving a known next-hop IPv4 address to its link address.

D - Incorrect: ICMP reports network errors and diagnostics rather than resolving hardware addresses.

Primary note proof

Study-note section NET20

> ARP resolves an on-link IPv4 next hop to a link address, using a broadcast request and normally unicast reply. For an off-subnet target, ARP resolves the gateway, not the remote target's MAC. It bridges the network/link addressing boundary and is often classified at the link layer; calling ARP simply a network protocol uses a loose textbook convention. RARP reverses hardware-to-IP lookup; BOOTP/DHCP support boot configuration. ICMP reports errors and diagnostics; IGMP manages IPv4 multicast membership. These are separate companion protocols, not four pieces whose combination is IP.

Study-note section NET20

> DNS resolves names to records, including IPv4 A and IPv6 AAAA addresses; it can use UDP or TCP port 53. DHCP dynamically leases IPv4 settings, commonly address, mask, gateway and DNS

server. Its basic exchange is discover, offer, request, acknowledge. IP itself does not assign addresses.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 17 | lines 44-53

ARP - Address Resolution Protocol: It is used to
resolve thephysical address of a device on a network,
where its logical address is known.
Physical address is the 48 bit address that is imprinted
on theNIC or LAN card, Logical address is the Internet
Address orcommonly known as IP address that is used
to uniquely & universally identify a device.
RARP- Reverse Address Resolution Protocol: It is
used bya device on the network to find its Internet
address when it knows its physical address.

Data Communication and Computer Networking module | PDF page 17 | lines 54-59

ICMP- Internet Control Message Protocol: It is a
signaling mechanism used to inform the sender about
datagram problemsthat occur during transit. It is used by
intermediate devices.
IGMP- Internet Group Message Protocol: It is a mechanism
that allows sending the same message to a group of recipients.

Data Communication and Computer Networking module | PDF page 28 | lines 32-45

Application Layer
The application layer in TCP/IP is equivalent to the
combined session, presentation, and application layers in
the OSI model and many protocols are defined at this
layer.
The Process/Application Layer Protocols
• Telnet
• File Transfer Protocol (FTP)
• Network File System (NFS).
• Simple Mail Transfer Protocol (SMTP
• POP3 is used to receive mail.
• Simple Network Management Protocol (SNMP)
• Domain Name Service (DNS)
• Dynamic Host Configuration Protocol (DHCP)

Question sources

MOE Computer Science Exit Exam · 2016 · Question 88

Question 10 | Q00089

A 172.16.0.0/16 parent network is divided into equal /19 broadcast subnets. Counting all subnets, which statement is correct?

A. It provides 8 subnets, 32 IP addresses each

B. It provides 8 subnets, 8,190 hosts each

C. It provides 8 subnets, 30 hosts each

D. It provides 8 subnets, 2,046 IP addresses each

Hint

Convert the mask to a prefix, separate network and host bits, and apply the relevant subnet-count or usable-host rule.

Answer B: It provides 8 subnets, 8,190 hosts each

Moving from /16 to /19 borrows three subnet bits, producing 2^3 = 8 equal subnets. Each /19 leaves thirteen host bits, so it contains 8192 addresses. Reserving the network and directed-broadcast addresses leaves 8190 usable hosts. Subnet counts describe subdivision of the stated parent; they must not be confused with addresses or hosts within a child subnet.

Why each choice is right or wrong

A - Incorrect: Eight subnets is correct, but each /19 has 8192 total addresses rather than 32.

B - Correct: Three borrowed bits yield eight subnets; thirteen host bits yield 8190 usable hosts per subnet.

C - Incorrect: Thirty usable hosts belongs to /27, not /19.

D - Incorrect: A /19 contains 8192 addresses, not 2046.

Primary note proof

Study-note section NET26

> To split parent /a into equal /p blocks, borrow b=p-a bits and obtain 2^b subnets. Do not subtract two subnets under modern practice. For a Class B /16 parent split to /19, b=3 gives eight subnets, each with 8192 addresses and 8190 conventional hosts. A /19 alone does not state its parent.

Study-note section NET25

> For ordinary broadcast LANs let h=32-p. Total addresses=2^h; usable hosts=2^h-2, reserving network and directed broadcast. Find the changing octet's increment as 256-mask octet, round the address down to a multiple, and extend through the next boundary minus one.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 18 | lines 45-54

> IP addresses: IP address uniquely identifies a device on the
> Internet. Every host and router on the Internet has an IP address,

which encodes its network number and host number.
• The combination is unique: in principle, no two machines on the Internet have the same IP address.
• An IPv4 address is 32 bits long
• They are used in the Source address and Destination address fields of IP packets.
• An IP address does not refer to a host but it refers to a network interface.

Data Communication and Computer Networking module | PDF page 19 | lines 2-22

Address Space: An address space is the total number ofaddresses used by the protocol.
• If a protocol uses N bits to define an address, the address space is 2N because each bit can have twodifferent values (0 or 1) and N bits can have 2N values.
• IPv4 uses 32-bit addresses, which means that the address space is 232 or 4,294,967,296 (more than 4billion).
Notations: There are two notations to show an IPv4 address:
• Binary notation: The IPv4 address is displayed as 32bits. ex. 11000001 10000011 00011011 11111111
• Dotted decimal notation: To make the IPv4 address easier to read, Internet addresses are usually written in decimal form with a decimal point (dot) separatingthe bytes. Each byte (octet) is 8 bits hence each number in dotted-decimal notation is a value rangingfrom 0 to 255. Ex. 129.11.11.239

Data Communication and Computer Networking module | PDF page 19 | lines 23-36

Classful addressing : In classful addressing, the addressspace is divided into five classes: A, B, C, D, and E.
• Netid and Hostid In classful addressing, an IP addressin class A, B, or C is divided into netid and hostid.
Subnetting: It allows a network to be split into several parts for internal use but still act like a single network to the outsideworld.
• To implement subnetting, the router needs a subnet mask that indicates the split between network + subnet number and host. Ex.

255.255.252.0/22. A‖/22‖ to indicate that the subnet mask is 22 bits long.

Question sources

MOE Computer Science Exit Exam · 2016 · Question 89

Question 11 | Q00090

A network device that provides the physical interface between computer and cabling is known as_____.

A. Switch

B. Router

C. NIC

D. Repeater

Hint

Compare signal repetition, frame forwarding, packet routing and policy enforcement using the stated device or traffic assumptions.

Answer C: NIC

The star-topology description places RJ-45 cable connections at the NIC of each computer; the physical address is imprinted on that NIC. This identifies the host cabling interface. Evidence: PDF 23, 17, 12, 12, 11.

Why each choice is right or wrong

A - Incorrect: A switch forwards among attached devices (PDF 23, 17, 12, 12, 11.)

B - Incorrect: A router interconnects networks (PDF 23, 17, 12, 12, 11.)

C - Correct: The module names Network Interface Card and connects cable to it (PDF 23, 17, 12, 12, 11.)

D - Incorrect: A repeater regenerates a signal on a LAN (PDF 23, 17, 12, 12, 11.)

Primary note proof

Study-note section NET09

A NIC supplies a computer’s network interface and commonly implements both physical and link functions. Calling a NIC a physical interface does not mean all its functions are layer 1. Physical specifications include connectors, signaling, voltage, timing and physical coding/modulation; the PHY interface to MAC handles hardware signaling.

Study-note section NET10

A bridge or ordinary Ethernet switch operates at layer 2. It learns source-MAC-to-port mappings, looks up the destination, forwards a known unicast to its port, filters it if the destination is on the

incoming segment, and floods an unknown unicast or broadcast within its VLAN. A switch does not always send only to one destination port. Wireless access points normally bridge wireless and wired link-layer traffic.

Study-note section NET11

Routers forward IP packets between networks using destination prefixes and next hops. They separate broadcast domains and normally do not forward local link broadcasts. A default gateway is usually a router, while a protocol gateway can translate application formats; therefore a gateway is not inherently a device that implements every OSI layer.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 23 | lines 19-34

Star Topology: in this topology, each node is connected directly to a central device called a hub or a switch. Data on a star network passes through the central device (switch) before continuing to its destination. The central device manages and controls all functions of the network. This configuration is common with twisted pair cable. RJ-45 Connectors are used to connect the cable to the Network Interface Card (NIC) of each computer. Its advantages include, ease of installation and reconfiguration, robust (ease of fault identification and isolation), link failure only affects device(s) connected to that link, and is less expensive than mesh. Its drawbacks include more cable requirements (than bus and ring) and single point of failure (if central device fail, the whole system will be down).

Data Communication and Computer Networking module | PDF page 17 | lines 44-53

ARP - Address Resolution Protocol: It is used to resolve thephysical address of a device on a network, where its logical address is known.
Physical address is the 48 bit address that is imprinted on theNIC or LAN card, Logical address is the Internet Address orcommonly known as IP address that is used to uniquely & universally identify a device.
RARP- Reverse Address Resolution Protocol: It is used bya device on the network to find its Internet address when it knows its physical address.

Data Communication and Computer Networking module | PDF page 12 | lines 38-52

ROUTER: Router is a specialized network device used tointerconnect different types of network that uses different protocol.

Router allows the users to connect several LAN and WAN
• A LAN to another LAN
• A WAN to another WAN
• A LAN to the Internet
Routers use the routing table to determine how to forwardpackets.
• The list of routing tables provides directions to transfer the data to a particular network destination -various paths to forward the data.
• A router analyzes a destination IP address of a givenpacket and compares it with the routing table to decide the packet's next best path

Data Communication and Computer Networking module | PDF page 12 | lines 27-37

SWITCH: A switch filters and forwards data packets across anetwork.
Unlike a hub which simply replicates what it receives on oneport onto all the other ports, a switch keeps a record of the MAC addresses of the devices attached to it.
When the switch receives a data packet, it forwards the packetdirectly to the recipient device by looking up the MAC address.
• Switch is intelligent and expensive than Hub
• Switch is a point to point communication device
• Hub is a broadcasting device

Data Communication and Computer Networking module | PDF page 11 | lines 54-55

Repeater: A repeater is a device that operates only in the physical layer. A repeater receives a signal and, before it

Question sources

MOE Computer Science Exit Exam · 2016 · Question 90

Question 12 | Q00141

In the OSI teaching model, which layers provide hop-local or end-to-end flow control and error recovery when the chosen protocols support them? Select all that apply; isolated header-error detection alone does not qualify.

A. Application

B. Presentation

C. Network

D. Transport

E. Session

F. Data link

G. Physical

Hint

Match the requested scope or data unit to the layer duties in the note; distinguish hop delivery from end-to-end process delivery.

Answer D, F: Transport; Data link

Data-link protocols can provide hop-local flow control and recovery, such as acknowledgments and retransmission. Transport protocols such as TCP provide end-to-end flow control and reliable delivery. These capabilities depend on the protocol: Ethernet detection alone does not guarantee recovery, and UDP does not provide TCP reliability. IPv4 checks its header but remains best-effort and does not supply the requested end-to-end recovery and flow-control service.

Why each choice is right or wrong

A - Incorrect: Application supplies application-facing network services, not the specified OSI control role.

B - Incorrect: Presentation concerns representation, compression and encryption roles.

C - Incorrect: IPv4 header checks detect some errors, but IP lacks the requested recovery and flow-control service.

D - Correct: Transport protocols such as TCP provide end-to-end flow control and recovery.

E - Incorrect: Session manages dialog and checkpoints rather than the specified delivery controls.

F - Correct: Data-link protocols can provide hop-local flow control and recovery.

G - Incorrect: Physical signaling transmits symbols rather than implementing these delivery-control procedures.

Primary note proof

Study-note section NET14

> Controlled access uses polling, reservations or a token to grant turns; correctly coordinated access avoids contention collisions. Channelization divides frequency, time or code resources. Stop-and-wait sends one frame and waits for ACK, retransmitting on timeout; sequence bits

distinguish duplicates. Sliding windows permit multiple unacknowledged frames. Link reliability/flow control is hop-local; transport reliability/flow control is end-to-end. Ethernet detects corruption but does not itself guarantee reliable delivery.

Study-note section NET17

TCP offers a reliable ordered byte stream using sequence numbers, acknowledgments, retransmission and windows. Flow control protects the receiver; congestion control protects network capacity. UDP sends independent datagrams with ports and a checksum but no built-in setup, delivery guarantee, retransmission or ordering. Live interactive traffic may choose UDP when late data is less useful than lost data. Application protocols can add reliability over UDP.

Study-note section NET19

OSI session roles establish/manage dialogs and can coordinate checkpoints so transfer resumes after interruption. Presentation roles translate encodings and handle compression/encryption. Compression reduces representation size; encryption hides content and need not shrink it. Application protocols provide services directly to applications. Practical implementations distribute these functions differently; TLS is not proof of a separate physical presentation-layer device.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 15 | lines 13-40

Data Link Layer
• The Data Link layer adds reliability to the physical layer by providing error detection and correction mechanisms.
• Framing: the Data Link layer receives the data from Network Layer and divides the stream of bits into fixed size manageable units called as Frames and sends it to the physical layer. On the receiver side, the data link layer receives the stream of bits from the physical layer and regroups them into frames and sends them to the Network layer.
• Physical Addressing: The Data link layer appends the physical address in the header of the frame before sending it to physical layer.
• Flow control: The data link layer makes sure that the sender sends the data at a speed at which the receiver canreceive it else if there is an overflow at the receiver sidethe data will be lost.
• Error Control: The data link layer imposes error control mechanism to identify lost or damaged frames, duplicateframes and then retransmit them.
• Access Control: The data link layer imposes access control mechanism to determine which device has right to send data in an multipoint

connection setting.
• Main Responsibility: The main responsibility of the data link layer is hop to hop transmission of frames.

Data Communication and Computer Networking module | PDF page 16 | lines 2-17

• At the sending side, the transport layer receives data from the session layer, divides it into units called segments and sends it to the network layer.
• To ensure process to process delivery the transport layer makes use of port address to identify the data from the sending and receiving process.
• The data can be transported in a connection oriented or connectionless manner.
• The Transport layer is responsible for segmentation and reassembly of the message into segments which bear sequence numbers.
• The transport layer also carries out flow control and error control functions; but unlike data link layer these are end to end rather than node to node.
• The main responsibility of the transport layer is process to process delivery of the entire message

Data Communication and Computer Networking module | PDF page 16 | lines 43-47

Application Layer
• The application layer enables the user to communicate its data to the receiver by providing certain services.
• The main Responsibility of Application layer is to provide the user access to network resources.

Data Communication and Computer Networking module | PDF page 16 | lines 33-42

Presentation Layer
• The communicating devices may be having different platforms. The presentation layer performs translation, encryption and compression of data.
• The presentation layer receives the data from the application layer adds header which contains information related to encryption and compression and sends it to the session layer.
• So, the main responsibility of the Presentation layer is translation, compression and encryption.

Data Communication and Computer Networking module | PDF page 15 | lines 41-61

Network Layer
• The network layer makes sure that the data is deliveredto the receiver despite multiple

intermediate devices.
• The network layer at the sending side accepts data from the transport layer, divides it into packets, addsaddressing information in the header and passes it tothe data link layer.
• The network layer is responsible for source todestination of delivery of data.
• The network layer uses logical address commonlyknown as IP address to recognize devices on the network.
• Each packet is independent of the other and may travelusing different routes to reach the receiver hence may arrive out of turn at the receiver (Routing).
• The Network layer does not perform any flow controlor error control
• The main responsibility of Network Layer is transmission of packets from source to destination

Data Communication and Computer Networking module | PDF page 14 | lines 32-49

Physical Layer:
• The Physical Layer provides a standardized interface to physical transmission media, including: Mechanical specification of electrical connectors and cables, for example maximum cable length, Electrical specification of transmission line and Bit-by-bit or symbol-by-symbol delivery.
• Interface: The Physical Layer defines the characteristics of interfaces between the devices & transmission medium.
• Representation of bits: The physical layer is concerned with transmission of signals from one device to another which involves converting data (1_s & 0_s) into signals and vice versa. It is not concerned with the meaning or interpretation of bits.
• Data rate: The physical layer defines the data transmission rate i.e. number of bits sent per second. It is the responsibility of the physical layer to maintain the defined data rate.

Question sources

Addis Ababa University mock exam · Question 43

Question 13 | Q00142

Which of the following statement(s) is/are WRONG? (Choose all that applies)

A. Internet/Network layer is responsible for routing

B. Physical address can be assigned by the network administrator.

C. Physical layer is concerned with specifying the characteristics of the transmission medium, the nature of the signals and the data rate.

D. Transport layer provides only unreliable data transmission.

E. Network layer is responsible for host to host communication.

F. None of the above

Hint

Use the cited note definitions to identify the requested function or scope, then check each alternative against that same rule.

Answer D: The transport layer does not provide only unreliable transmission

The question asks for WRONG statements. TCP is a transport-layer protocol with reliable ordered delivery, disproving the absolute “only unreliable” in D. The other substantive statements fit the layer model: network routing and host delivery, physical signaling specifications, and administratively assigned MAC addresses. NET33 explicitly permits locally administered MAC addresses, so B must not be rejected.

Why each choice is right or wrong

A - Incorrect: This statement is true: routing is a network/Internet-layer responsibility, so it is not a wrong statement.

B - Incorrect: NET33 permits locally administered MAC addresses; physical addresses need not always be factory assigned.

C - Incorrect: Physical signaling, transmission-medium characteristics and data rate belong to the physical layer.

D - Correct: The word only is false: TCP supplies reliable transport, whereas UDP lacks built-in delivery guarantees.

E - Incorrect: Host-to-host packet delivery is a network-layer function, distinct from transport process delivery.

F - Incorrect: At least D is wrong, so none of the above cannot answer the requested negative test.

Primary note proof

Study-note section NET33

> First identify the exact layer, protocol and scope. Flow/error control can exist at both link and transport layers; MAC addresses can be locally administered; bridges and switches both operate at layer 2. A LAN can use public or private unicast space. UDP and IP are both connectionless. Session dialogs and TCP connections are distinct senses of connection. Distinguish the protocol, layer and scope before treating these descriptions as exclusive.

Study-note section NET17

TCP offers a reliable ordered byte stream using sequence numbers, acknowledgments, retransmission and windows. Flow control protects the receiver; congestion control protects network capacity. UDP sends independent datagrams with ports and a checksum but no built-in setup, delivery guarantee, retransmission or ordering. Live interactive traffic may choose UDP when late data is less useful than lost data. Application protocols can add reliability over UDP.

Study-note section NET09

A NIC supplies a computer's network interface and commonly implements both physical and link functions. Calling a NIC a physical interface does not mean all its functions are layer 1. Physical specifications include connectors, signaling, voltage, timing and physical coding/modulation; the PHY interface to MAC handles hardware signaling.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 15 | lines 41-61

Network Layer
• The network layer makes sure that the data is deliveredto the receiver despite multiple intermediate devices.
• The network layer at the sending side accepts data from the transport layer, divides it into packets, addsaddressing information in the header and passes it tothe data link layer.
• The network layer is responsible for source todestination of delivery of data.
• The network layer uses logical address commonlyknown as IP address to recognize devices on the network.
• Each packet is independent of the other and may travelusing different routes to reach the receiver hence may arrive out of turn at the receiver (Routing).
• The Network layer does not perform any flow controlor error control
• The main responsibility of Network Layer is transmission of packets from source to destination

Data Communication and Computer Networking module | PDF page 14 | lines 32-49

Physical Layer:
• The Physical Layer provides a standardized interface to physical transmission media, including: Mechanical specification of electrical connectors and cables, for example maximum cable length, Electrical specification of transmission line and Bit-by-bit or symbol-by-symbol delivery.

• Interface: The Physical Layer defines the characteristics of interfaces between the devices & transmission medium.
• Representation of bits: The physical layer is concerned with transmission of signals from one device to another which involves converting data (1_s & 0_s) into signals and vice versa. It is not concerned with the meaning or interpretation of bits.
• Data rate: The physical layer defines the data transmission rate i.e. number of bits sent per second. It is the responsibility of the physical layer to maintain the defined data rate.

Data Communication and Computer Networking module | PDF page 18 | lines 9-21

TCP - Transmission Control Protocol: TCP is a reliable connection-oriented, reliable protocol. i.e. a connection is established between the sender and receiver before the data can be transmitted. It divides the data it receives from the upper layer into segments and tags a sequence number to each segment which is used at the receiving end for reordering of data.
UDP - User Datagram Protocol: UDP is a simple protocol used for process to process transmission. It is an unreliable, connectionless protocol for applications that do not require flow control or error control. It simply adds port address, checksum and length information to the data it receives from the upper layer.

Data Communication and Computer Networking module | PDF page 17 | lines 44-53

ARP - Address Resolution Protocol: It is used to resolve thephysical address of a device on a network, where its logical address is known.
Physical address is the 48 bit address that is imprinted on theNIC or LAN card, Logical address is the Internet Address orcommonly known as IP address that is used to uniquely & universally identify a device.
RARP- Reverse Address Resolution Protocol: It is used bya device on the network to find its Internet address when it knows its physical address.

Question sources

Addis Ababa University mock exam · Question 44

Question 14 | Q00143

Which one of the following Medium Access Control protocols is supported by WLAN (802.11)?

A. ALOHA

B. CSMA/CA

C. Token Passing

D. FDMA

E. CSMA

Hint

Compare the signal mechanism, medium properties or transmission direction against the definitions and stated physical assumptions.

Answer B: CSMA/CA

NET14 names CSMA/CA as the 802.11 Wi-Fi access procedure. It combines carrier sensing, waiting/backoff and acknowledgments rather than Ethernet-style collision detection or token turns. Generic CSMA describes its family, but B gives the specifically supported WLAN mechanism requested by the stem; E omits its collision-avoidance procedure.

Why each choice is right or wrong

A - Incorrect: ALOHA sends opportunistically and is not the 802.11 contention mechanism identified in NET14.

B - Correct: CSMA/CA is the specifically identified WLAN mechanism, using waiting/backoff and acknowledgments.

C - Incorrect: Token passing is controlled access, unlike the contention procedure used by ordinary 802.11 WLANs.

D - Incorrect: FDMA divides frequency resources; it is not the stated WLAN medium-access protocol.

E - Incorrect: CSMA names the broader carrier-sensing family but omits the specific collision-avoidance WLAN protocol offered in B.

Primary note proof

Study-note section NET14

> Random access allows contention: ALOHA sends opportunistically; CSMA senses before sending. In legacy half-duplex Ethernet, CSMA/CD detects collision, sends a jam indication, stops, and retries after random backoff. The jam signals a collision, not its clearance. Wi-Fi 802.11 uses CSMA/CA with waiting/backoff and acknowledgments; sensing does not eliminate hidden-terminal collisions.

Study-note section NET14

Controlled access uses polling, reservations or a token to grant turns; correctly coordinated access avoids contention collisions. Channelization divides frequency, time or code resources. Stop-and-wait sends one frame and waits for ACK, retransmitting on timeout; sequence bits distinguish duplicates. Sliding windows permit multiple unacknowledged frames. Link reliability/flow control is hop-local; transport reliability/flow control is end-to-end. Ethernet detects corruption but does not itself guarantee reliable delivery.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 21 | lines 6-26

MEDIUM ACCESS CONTROL
The problem of controlling the access to the medium is similarto the rules of speaking in a meeting (the right to speak isupheld; two people do not speak at the same time; do notinterrupt each other; do not monopolize the discussion; ...) Three categories of multiple access protocols
Random Access Protocols - try your best like taxis do
• MA - Multiple Access
• CSMA - Carrier Sense MA
• CSMA/CD - CSMA with Collision Detection
• CSMA/CA - CSMA with Collision AvoidanceControlled-Access Protocols - get permission
• Reservation
• Polling
• Token Passing
Channelization Protocols - simultaneous use
• FDMA - Frequency-Division MA
• TDMA - Time-Division MA
• CDMA - Code-Division MA

Question sources

Addis Ababa University mock exam · Question 45

Question 15 | Q00144

Which device category can perform protocol conversion at higher OSI layers, potentially including application formats, rather than being limited to basic repeating, MAC bridging or IP routing?

A. Hub

B. Switch

C. Router

D. Gateway

E. Bridge

Hint

Match the requested scope or data unit to the layer duties in the note; distinguish hop delivery from end-to-end process delivery.

Answer D: Gateway

A protocol gateway translates between protocol or application representations, so its possible scope extends above basic link forwarding and IP routing. A hub repeats signals, a basic switch or bridge forwards using link-layer information, and a basic router forwards IP packets. Gateway is used in several senses: an ordinary default gateway is usually a router and need not implement conversion across every OSI layer.

Why each choice is right or wrong

A - Incorrect: A hub repeats physical signals rather than converting application protocols.

B - Incorrect: A basic layer-2 switch forwards frames by link-layer information.

C - Incorrect: A basic router chooses IP next hops rather than translating application formats.

D - Correct: A protocol-conversion gateway can translate higher-layer formats.

E - Incorrect: A bridge forwards between links using MAC information rather than higher-layer protocol conversion.

Primary note proof

Study-note section NET11

> Routers forward IP packets between networks using destination prefixes and next hops. They separate broadcast domains and normally do not forward local link broadcasts. A default gateway is usually a router, while a protocol gateway can translate application formats; therefore a gateway is not inherently a device that implements every OSI layer.

Study-note section NET09

> A repeater regenerates layer-1 signals without inspecting destination addresses. An active hub is a multiport repeater: it repeats incoming signals onto other ports, placing half-duplex endpoints in one collision domain. A passive hub is a connector. A hub neither learns MAC addresses nor

eliminates collisions. An endpoint such as a network printer consumes services; routers, hubs and access points are intermediary devices.

Study-note section NET10

A bridge or ordinary Ethernet switch operates at layer 2. It learns source-MAC-to-port mappings, looks up the destination, forwards a known unicast to its port, filters it if the destination is on the incoming segment, and floods an unknown unicast or broadcast within its VLAN. A switch does not always send only to one destination port. Wireless access points normally bridge wireless and wired link-layer traffic.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 12 | lines 17-26

Active Hubs
An active hub is actually a multipart repeater. It is normallyused to create connections between stations in a physical startopology.
HUB: Hubs are commonly used to connect segments (devices)of a LAN. Hubs don‘t filter information; instead broadcast incoming packets to all computers connected to it. A hub contains multiple ports which support 8, 12 or 24 RJ-45 ports. Two types: Passive hub and Active hub. It is used in star or ring topology.

Data Communication and Computer Networking module | PDF page 12 | lines 27-37

SWITCH: A switch filters and forwards data packets across anetwork.
Unlike a hub which simply replicates what it receives on oneport onto all the other ports, a switch keeps a record of the MAC addresses of the devices attached to it.
When the switch receives a data packet, it forwards the packetdirectly to the recipient device by looking up the MAC address.
• Switch is intelligent and expensive than Hub
• Switch is a point to point communication device
• Hub is a broadcasting device

Data Communication and Computer Networking module | PDF page 12 | lines 38-52

ROUTER: Router is a specialized network device used tointerconnect different types of network that uses different protocol.
Router allows the users to connect several LAN and WAN
• A LAN to another LAN
• A WAN to another WAN
• A LAN to the Internet
Routers use the routing table to determine how to

forwardpackets.
• The list of routing tables provides directions to transfer the data to a particular network destination -various paths to forward the data.
• A router analyzes a destination IP address of a givenpacket and compares it with the routing table to decide the packet's next best path

Data Communication and Computer Networking module | PDF page 49 | lines 34-37

Gateways are basically protocol converters, facilitating compatibility between two protocols and operating on any layer of the open systems interconnection (OSI) model.

Data Communication and Computer Networking module | PDF page 12 | lines 60-61

BRIDGE: Connects two LANS having the same protocol - (e.g. Ethernet or Token ring).

Question sources

Addis Ababa University mock exam · Question 46

Question 16 | Q00145

Which listed address can be assigned as an RFC1918 private unicast host address on a correctly configured /24 LAN? Select one.

A. 127.0.0.0

B. 9.0.0.1

C. 192.168.1.256

D. 172.16.1.27

E. All of the above

F. None of the above

Hint

Convert the mask to a prefix, separate network and host bits, and apply the relevant subnet-count or usable-host rule.

Answer D: 172.16.1.27

An ordinary host address must have valid octets, belong to the required address scope and avoid the subnet network and broadcast addresses. The address 172.16.1.27 belongs to private 172.16.0.0/12 and is an interior host of 172.16.1.0/24. The public address 9.0.0.1 does not meet the private-address requirement. Loopback and an octet of 256 fail the other checks.

Why each choice is right or wrong

A - Incorrect: 127/8 is reserved for loopback and is not an ordinary LAN interface assignment.

B - Incorrect: 9.0.0.1 is public unicast, so it fails the explicit RFC1918 private-address requirement.

C - Incorrect: An IPv4 octet must be 0-255; 256 makes this address syntactically invalid.

D - Correct: 172.16.1.27 is within private 172.16/12 and is neither the network nor broadcast of its /24.

E - Incorrect: All fails because loopback and the impossible .256 octet are not valid ordinary LAN host assignments.

F - Incorrect: A private usable host is offered, so none of the above is false.

Primary note proof

Study-note section NET23

RFC1918 private blocks are 10.0.0.0/8, 172.16.0.0/12 (through 172.31.255.255), and 192.168.0.0/16. They can be reused internally but are not globally routed as public destinations. A LAN may also use legitimately assigned public addresses; private is common, not mandatory. 127.0.0.0/8 is IPv4 loopback, commonly 127.0.0.1, for local protocol access without an external link. 255.255.255.255 is limited broadcast; 0.0.0.0 can identify an unconfigured source. Link-local/APIPA uses 169.254.0.0/16, with edge /24 blocks excluded from normal automatic selection.

Study-note section NET25

For ordinary broadcast LANs let h=32-p. Total addresses=2^h; usable hosts=2^h-2, reserving network and directed broadcast. Find the changing octet's increment as 256-mask octet, round the address down to a multiple, and extend through the next boundary minus one.

Study-note section NET22

Write IPv4 as four decimal octets 0-255, or as 32 binary bits. Use weights 128,64,32,16,8,4,2,1 within each octet. Thus 11000001 10000011 00011011 11111111 is 193.131.27.255. A value such as 257 is impossible. Syntactic validity differs from assignability: an address ending .0 or .255 can be a host under some prefixes.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 19 | lines 2-22

Address Space: An address space is the total
number ofaddresses used by the protocol.
• If a protocol uses N bits to define an address,
the address space is 2N
because each bit can
have twodifferent values (0 or 1) and N bits
can have 2N values.
• IPv4 uses 32-bit addresses, which means that
the address space is 232 or 4,294,967,296
(more than 4billion).

Notations: There are two notations to show an IPv4 address:
• Binary notation: The IPv4 address is displayed as 32bits. ex. 11000001 10000011 00011011 11111111
• Dotted decimal notation: To make the IPv4 address easier to read, Internet addresses are usually written in decimal form with a decimal point (dot) separatingthe bytes. Each byte (octet) is 8 bits hence each number in dotted-decimal notation is a value rangingfrom 0 to 255. Ex. 129.11.11.239

Data Communication and Computer Networking module | PDF page 19 | lines 45-49

NAT (Network Address Translation): The scarcity of network addresses in IPv4 led to the development of IPv6. Due to this, we need to use private IP address inside the organization and translate it to public IP address using NAT.

Data Communication and Computer Networking module | PDF page 65 | lines 31-38

/etc/hosts
The /etc/hosts file always contains the localhost IP address, 127.0.0.1, which is usedfor interprocess communication.
Never remove this line! Sometimes contains addresses of additional hosts, whichcan be contacted without using an external naming service such as DNS (the Domain Name Server).

Question sources

Addis Ababa University mock exam · Question 47

Question 17 | Q00146

For the switching methods below, select all statements that are correct. In D, allocation on demand means reservation when a circuit is established.

A. Circuit Switching and Virtual Packet Switching methods reserve the required resources for the duration of the session during communication between end systems

B. Circuit switching technique uses store and forward method.

C. In message switching technique, it is not required to create a dedicated path.

D. In circuit switching techniques, resources are allocated on demand.

E. Packet switching can have nonuniform delay because packets share links and may queue.

Hint

Compare signal repetition, frame forwarding, packet routing and policy enforcement using the stated device or traffic assumptions.

Answer C, D, E: In message switching technique, it is not required to create a dedicated path.; In circuit switching techniques, resources are allocated on demand.; Packet switching can have nonuniform delay because packets share links and may queue.

Message switching stores and forwards whole messages without a dedicated end-to-end path. Circuit switching instead reserves resources when a call is established and retains them through the session. Packet switching shares links, so queueing can produce variable delay, although packet voice remains possible. Virtual-circuit forwarding state alone does not require resource reservation. These distinctions support the three selected statements without equating all connection-oriented methods.

Why each choice is right or wrong

A - Incorrect: Circuit switching reserves resources, but virtual-circuit packet switching need not reserve them throughout a session.

B - Incorrect: Circuit switching uses an established reserved path; complete-message or packet buffering describes store-and-forward switching.

C - Correct: Message switching forwards stored messages without requiring a dedicated end-to-end circuit.

D - Correct: Circuit resources are allocated when a connection is requested and reserved for its session.

E - Correct: Shared links and queueing can give packets different delays.

Primary note proof

Study-note section NET31

> Circuit switching sets up a path with reserved resources, transfers data, then releases it. Predictable allocated bandwidth trades against setup/blocking and wasted reservation during silence. A traditional telephone call is the standard example. Packet switching divides data into packets that share links statistically; queueing can add variable delay and loss. This does not make modern voice-over-packet impossible: buffering, scheduling and capacity planning manage it.

Study-note section NET31

> Datagram packets are forwarded independently. Virtual circuits establish forwarding state, but resource reservation is optional, not a necessary property of every virtual circuit. Message switching stores a complete message before forwarding, without a dedicated end-to-end path. Packet store-and-forward waits for the full packet/frame; cut-through starts after enough header arrives; fragment-free historically waits through the initial collision-sensitive portion. No routing algorithm guarantees that every packet always takes the geometrically shortest route.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 20 | lines 12-26

Circuit Switching: In circuit switching, two communicating stations are connected by a dedicated communication path which consists of intermediate nodes in the network and the links that connect these nodes.
It involved the following three distinct steps
• Circuit Establishment: To establish an end-to-end connection before any transfer of data.
• Data transfer: Transfer data is from the source to the destination. The data may be analog or digital, depending on the nature of the network. The connection is generally full-duplex.
• Circuit disconnect: Terminate connection at the end of data transfer. Signals must be propagated to deallocate the dedicated resources.

Data Communication and Computer Networking module | PDF page 20 | lines 27-36

Message Switching:
Packet Switching: Packet switching was designed to address the shortcomings of circuit switching in dealing with data communication. Unlike circuit switching where communication is continuous along a dedicated circuit, in packet switching, communication is discrete in form of packets.
The three switching modes to choose from are:
• Cut-through
• Store-and-forward
• Fragment-free

Question sources

Addis Ababa University mock exam · Question 48

Question 18 | Q00147

Which information is not correct about the IP address 172.16.35.72/27?

A. 172.16.35.64 is one of the subnet addresses.

B. The default mask for the network is 255.255.0.0.

C. Itis Class B address.

D. The number of bits used for the host address is 5.

E. The broadcast address of the second subnet is 172.16.35.255

Hint

Convert the mask to a prefix, separate network and host bits, and apply the relevant subnet-count or usable-host rule.

Answer E: The claimed second-subnet broadcast is wrong

For /27, five host bits give blocks of 32 in the last octet. The block containing .72 is .64-.95, with broadcast .95. If second subnet means the second /27 inside .35.0/24, its broadcast is .63; neither reading gives .255. The historical class is B and default mask /16, although the actual subnet mask is /27.

Why each choice is right or wrong

A - Incorrect: The .64 boundary is a valid /27 subnet start and contains host .72.

B - Incorrect: As a historical Class B address, its default mask is /16, even though the supplied actual prefix is /27.

C - Incorrect: First octet 172 is in the historical Class B range 128-191.

D - Incorrect: A 32-bit IPv4 address with /27 leaves exactly five bits for the host portion.

E - Correct: The second /27 in the local /24 broadcasts at .63; the containing subnet broadcasts at .95, never .255.

Primary note proof

Study-note section NET25

> For ordinary broadcast LANs let h=32-p. Total addresses=2^h; usable hosts=2^h-2, reserving network and directed broadcast. Find the changing octet's increment as 256-mask octet, round the address down to a multiple, and extend through the next boundary minus one.

Study-note section NET22

> Historical classes use leading patterns: A 0 with /8, B 10 with /16, C 110 with /24; D 1110 is multicast and E 1111 reserved. Ordinary class-A first octets are 1-126 because 0 and 127 have special uses. B spans 128-191 and C 192-223. Default usable counts are 2^24-2, 2^16-2 and 254. Modern CIDR requires the actual prefix and overrides class defaults.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 18 | lines 45-54

> IP addresses: IP address uniquely identifies a device on the
> Internet. Every host and router on the Internet has an IP address,
> which encodes its network number and host number.
> • The combination is unique: in principle, no two
> machines on the Internet have the same IP address.
> • An IPv4 address is 32 bits long
> • They are used in the Source address and Destination
> address fields of IP packets.

• An IP address does not refer to a host but it refers to a network interface.

Data Communication and Computer Networking module | PDF page 19 | lines 2-22

Address Space: An address space is the total number ofaddresses used by the protocol.
• If a protocol uses N bits to define an address, the address space is 2N because each bit can have twodifferent values (0 or 1) and N bits can have 2N values.
• IPv4 uses 32-bit addresses, which means that the address space is 232 or 4,294,967,296 (more than 4billion).
Notations: There are two notations to show an IPv4 address:
• Binary notation: The IPv4 address is displayed as 32bits. ex. 11000001 10000011 00011011 11111111
• Dotted decimal notation: To make the IPv4 address easier to read, Internet addresses are usually written in decimal form with a decimal point (dot) separatingthe bytes. Each byte (octet) is 8 bits hence each number in dotted-decimal notation is a value rangingfrom 0 to 255. Ex. 129.11.11.239

Data Communication and Computer Networking module | PDF page 19 | lines 23-36

Classful addressing : In classful addressing, the addressspace is divided into five classes: A, B, C, D, and E.
• Netid and Hostid In classful addressing, an IP addressin class A, B, or C is divided into netid and hostid.
Subnetting: It allows a network to be split into several parts for internal use but still act like a single network to the outsideworld.
• To implement subnetting, the router needs a subnet mask that indicates the split between network + subnet number and host. Ex. 255.255.252.0/22. A‖/22‖ to indicate that the subnet mask is 22 bits long.

Question sources

Addis Ababa University mock exam · Question 49

Question 19 | Q00156

Which one of the following is false about HTTP protocol?

A. Itis a stateless protocol

B. An HTTP message body can be empty

C. Itis a protocol used for communication between a web browser and a web server

D. None of the above

Hint

Identify the requested service or delivery guarantee, then distinguish application roles, transport behavior and address configuration.

Answer D: None of the listed HTTP claims is false

All three substantive choices agree with NET21: HTTP is stateless, a message body may be absent, and HTTP defines web request/response exchanges such as those between browsers and servers. The negative stem therefore has no false statement among A-C; D is the offered none-of-the-above response.

Why each choice is right or wrong

A - Incorrect: Statelessness is an HTTP property given in NET21, so this statement is true rather than false.

B - Incorrect: An HTTP message can omit its body, making this statement true.

C - Incorrect: Browser-to-web-server requests and responses are an ordinary use of HTTP, consistent with its web semantics.

D - Correct: A, B and C are all true, so none supplies the false statement requested.

Primary note proof

Study-note section NET21

> HTTP defines web request/response semantics; it is stateless, and a message body may be absent. HTTPS adds TLS protection. FTP transfers files using control and separate data connections; it is not the same protocol as SFTP. SMTP submits and relays mail; POP3 retrieves messages and IMAP accesses/synchronizes server mailboxes. Saying SMTP handles both sending and end-user mailbox retrieval is inaccurate.

Study-note section NET21

> Usual service ports: FTP control 21, SSH 22, Telnet 23, SMTP relay 25, DNS 53, HTTP 80, POP3 110, IMAP 143, HTTPS 443. Telnet provides unencrypted remote terminals; SSH protects remote access. Servers can be configured on other ports. A browser's HTTP exchange does not determine the physical duplex mode of its network interface.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 28 | lines 23-31

Telnet 23 SNMP 161
SMTP 25 TFTP 69
HTTP 80 DNS 53
FTP 21 POP3 110
DNS 53 DHCP 68
HTTPS 443 NTP 123
SSH 22 RPC 530
Table. Sample TCP and UDP port numbers from well-known category

Data Communication and Computer Networking module | PDF page 28 | lines 32-45

Application Layer
The application layer in TCP/IP is equivalent to the combined session, presentation, and application layers in the OSI model and many protocols are defined at this layer.
The Process/Application Layer Protocols
• Telnet
• File Transfer Protocol (FTP)
• Network File System (NFS).
• Simple Mail Transfer Protocol (SMTP
• POP3 is used to receive mail.
• Simple Network Management Protocol (SNMP)
• Domain Name Service (DNS)
• Dynamic Host Configuration Protocol (DHCP)

Question sources

Addis Ababa University mock exam · Question 58

Question 20 | Q00204

POP3 is most commonly used for:

A. Managing devices (such as routers and switches) on a network

B. Mapping IP addresses to hardware addresses

C. Sending emails from an email client to an email server

D. Retrieving emails from an email server to an email client

Hint

Use the cited note definitions to identify the requested function or scope, then check each alternative against that same rule.

Answer D: Retrieving emails from an email server to an email client

The module explicitly says POP3 is used to receive mail. Retrieval from a mail server into a client is that receiving function. Evidence: PDF 28, 17, 18.

Why each choice is right or wrong

A - Incorrect: Management is associated with SNMP, not POP3 (PDF 28, 17, 18.)

B - Incorrect: Address-to-hardware mapping is ARP (PDF 28, 17, 18.)

C - Incorrect: Sending mail is the SMTP role (PDF 28, 17, 18.)

D - Correct: Receiving mail matches the explicit POP3 statement (PDF 28, 17, 18.)

Primary note proof

Study-note section NET21

HTTP defines web request/response semantics; it is stateless, and a message body may be absent. HTTPS adds TLS protection. FTP transfers files using control and separate data connections; it is not the same protocol as SFTP. SMTP submits and relays mail; POP3 retrieves messages and IMAP accesses/synchronizes server mailboxes. Saying SMTP handles both sending and end-user mailbox retrieval is inaccurate.

Study-note section NET-S02

SNMP means Simple Network Management Protocol. Its management applications monitor and control managed devices, such as hosts and routers, by exchanging management information with their agents. This device-management role differs from transferring email, resolving names or mapping an IP address to a MAC address.

Study-note section NET20

ARP resolves an on-link IPv4 next hop to a link address, using a broadcast request and normally unicast reply. For an off-subnet target, ARP resolves the gateway, not the remote target's MAC. It bridges the network/link addressing boundary and is often classified at the link layer; calling ARP simply a network protocol uses a loose textbook convention. RARP reverses hardware-to-IP lookup; BOOTP/DHCP support boot configuration. ICMP reports errors and diagnostics; IGMP manages IPv4 multicast membership. These are separate companion protocols, not four pieces whose combination is IP.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 28 | lines 32-45

Application Layer
The application layer in TCP/IP is equivalent to the
combined session, presentation, and application layers in
the OSI model and many protocols are defined at this
layer.
The Process/Application Layer Protocols
• Telnet
• File Transfer Protocol (FTP)
• Network File System (NFS).
• Simple Mail Transfer Protocol (SMTP
• POP3 is used to receive mail.
• Simple Network Management Protocol (SNMP)

• Domain Name Service (DNS)
• Dynamic Host Configuration Protocol (DHCP)

Data Communication and Computer Networking module | PDF page 17 | lines 44-53

ARP - Address Resolution Protocol: It is used to resolve thephysical address of a device on a network, where its logical address is known.
Physical address is the 48 bit address that is imprinted on theNIC or LAN card, Logical address is the Internet Address orcommonly known as IP address that is used to uniquely & universally identify a device.
RARP- Reverse Address Resolution Protocol: It is used bya device on the network to find its Internet address when it knows its physical address.

Data Communication and Computer Networking module | PDF page 18 | lines 27-32

Application Layer
The Application Layer is a combination of Session, Presentation & Application Layers of OSI models and defines high level protocols like File Transfer (FTP), Electronic Mail (SMTP), Virtual Terminal (TELNET), Domain Name Service (DNS), etc.

Question sources

Mock exam 4 · Question 6

Question 21 | Q00205

The Address Resolution Protocol maps addresses between which layers?

A. Application layer to Network layer

B. Application layer to Transport layer

C. Transport layer to Network layer

D. Transport layer to Data link layer

E. Network layer to Data link layer

Hint

Match the requested scope or data unit to the layer duties in the note; distinguish hop delivery from end-to-end process delivery.

Answer E: Network layer to Data link layer

ARP takes a logical IP address and resolves the physical MAC address, connecting network addressing to data-link addressing. Evidence: PDF 17, 15, 15.

Why each choice is right or wrong

A - Incorrect: Application to network omits the MAC destination of the mapping (PDF 17, 15, 15.)

B - Incorrect: Application to transport is not IP-to-MAC resolution (PDF 17, 15, 15.)

C - Incorrect: Transport ports are not the known IP address (PDF 17, 15, 15.)

D - Incorrect: Transport to data link incorrectly starts with ports (PDF 17, 15, 15.)

E - Correct: Network IP to data-link physical address matches both ends (PDF 17, 15, 15.)

Primary note proof

Study-note section NET20

> ARP resolves an on-link IPv4 next hop to a link address, using a broadcast request and normally unicast reply. For an off-subnet target, ARP resolves the gateway, not the remote target's MAC. It bridges the network/link addressing boundary and is often classified at the link layer; calling ARP simply a network protocol uses a loose textbook convention. RARP reverses hardware-to-IP lookup; BOOTP/DHCP support boot configuration. ICMP reports errors and diagnostics; IGMP manages IPv4 multicast membership. These are separate companion protocols, not four pieces whose combination is IP.

Study-note section NET17

> Ports identify transport endpoints; the application can choose a transport and request socket buffer sizes, subject to OS limits. A TCP connection is identified by source/destination IP and source/destination port, with TCP understood. IPv4 protocol numbers identify upper protocols; 80 is a usual HTTP port, not an IP protocol number. Clients often use ephemeral ports. SCTP is a reliable message-oriented transport with multiple streams.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 17 | lines 44-53

> ARP - Address Resolution Protocol: It is used to
> resolve thephysical address of a device on a network,
> where its logical address is known.
> Physical address is the 48 bit address that is imprinted
> on theNIC or LAN card, Logical address is the Internet
> Address orcommonly known as IP address that is used
> to uniquely & universally identify a device.
> RARP- Reverse Address Resolution Protocol: It is
> used bya device on the network to find its Internet
> address when it knows its physical address.

Data Communication and Computer Networking module | PDF page 15 | lines 41-61

> Network Layer
> • The network layer makes sure that the data is
> deliveredto the receiver despite multiple
> intermediate devices.

• The network layer at the sending side accepts data from the transport layer, divides it into packets, addsaddressing information in the header and passes it tothe data link layer.
• The network layer is responsible for source todestination of delivery of data.
• The network layer uses logical address commonlyknown as IP address to recognize devices on the network.
• Each packet is independent of the other and may travelusing different routes to reach the receiver hence may arrive out of turn at the receiver (Routing).
• The Network layer does not perform any flow controlor error control
• The main responsibility of Network Layer is transmission of packets from source to destination

Data Communication and Computer Networking module | PDF page 15 | lines 13-40

Data Link Layer
• The Data Link layer adds reliability to the physical layer by providing error detection and correction mechanisms.
• Framing: the Data Link layer receives the data from Network Layer and divides the stream of bits into fixed size manageable units called as Frames and sends it to the physical layer. On the receiver side, the data link layer receives the stream of bits from the physical layer and regroups them into frames and sends them to the Network layer.
• Physical Addressing: The Data link layer appends the physical address in the header of the frame before sending it to physical layer.
• Flow control: The data link layer makes sure that the sender sends the data at a speed at which the receiver canreceive it else if there is an overflow at the receiver sidethe data will be lost.
• Error Control: The data link layer imposes error control mechanism to identify lost or damaged frames, duplicateframes and then retransmit them.
• Access Control: The data link layer imposes access control mechanism to determine which device has right to send data in an multipoint connection setting.
• Main Responsibility: The main responsibility of

the data link layer is hop to hop transmission of frames.

Question sources

Mock exam 4 · Question 7

Question 22 | Q00206

What is the first usable host addressing of prefix 172.105.180.0/21?

A. 172.105.180.1

B. 172.105.170.1

C. 172.105.175.1

D. 172.105.176.1

E. 172.105.172.1

Hint

Convert the mask to a prefix, separate network and host bits, and apply the relevant subnet-count or usable-host rule.

Answer D: 172.105.176.1

A /21 mask is 255.255.248.0, giving third-octet blocks of eight. 180 lies in the 176-183 block; masking therefore yields network 172.105.176.0, not 172.105.180.0. The first usable ordinary host is one address above the network boundary: 172.105.176.1. NET24 explicitly explains this unaligned host/prefix example.

Why each choice is right or wrong

A - Incorrect: This address is inside the block but is not its first usable address; the block begins at third octet 176.

B - Incorrect: Third octet 170 lies below the 176-183 range of the actual /21 block.

C - Incorrect: Third octet 175 is outside the block, immediately below its network boundary.

D - Correct: The network is 172.105.176.0/21, so its first usable ordinary host is 172.105.176.1.

E - Incorrect: Third octet 172 belongs to a different /21 block and is outside the specified network.

Primary note proof

Study-note section NET24

Compute network=address AND mask. Host bits zero identify the block start; host bits one give broadcast. With 172.16.28.252/20, the third octet is grouped in blocks of 16, so the network is 172.16.16.0 and broadcast 172.16.31.255. A written host/prefix such as 172.105.180.0/21 need not be an aligned block label: masking yields 172.105.176.0/21.

Study-note section NET25

For ordinary broadcast LANs let h=32-p. Total addresses=2^h; usable hosts=2^h-2, reserving network and directed broadcast. Find the changing octet's increment as 256-mask octet, round the address down to a multiple, and extend through the next boundary minus one.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 18 | lines 45-54

IP addresses: IP address uniquely identifies a device on the
Internet. Every host and router on the Internet has an IP address,
which encodes its network number and host number.
• The combination is unique: in principle, no two
machines on the Internet have the same IP address.
• An IPv4 address is 32 bits long
• They are used in the Source address and Destination
address fields of IP packets.
• An IP address does not refer to a host but it refers to a
network interface.

Data Communication and Computer Networking module | PDF page 19 | lines 2-22

Address Space: An address space is the total
number ofaddresses used by the protocol.
• If a protocol uses N bits to define an address,
the address space is 2N
because each bit can
have twodifferent values (0 or 1) and N bits
can have 2N values.
• IPv4 uses 32-bit addresses, which means that
the address space is 232 or 4,294,967,296
(more than 4billion).
Notations: There are two notations to show an IPv4 address:
• Binary notation: The IPv4 address is displayed
as 32bits. ex. 11000001 10000011 00011011
11111111
• Dotted decimal notation: To make the IPv4
address easier to read, Internet addresses are
usually written in decimal form with a decimal
point (dot) separatingthe bytes. Each byte (octet)
is 8 bits hence each number in dotted-decimal
notation is a value rangingfrom 0 to 255. Ex.
129.11.11.239

Data Communication and Computer Networking module | PDF page 19 | lines 23-36

Classful addressing : In classful addressing, the
addressspace is divided into five classes: A, B, C,
D, and E.
• Netid and Hostid In classful addressing, an IP

addressin class A, B, or C is divided into netid
and hostid.
Subnetting: It allows a network to be split into several
parts for internal use but still act like a single network to
the outsideworld.
• To implement subnetting, the router needs a
subnet mask that indicates the split between
network + subnet number and host. Ex.
255.255.252.0/22. A‖/22‖ to indicate that the
subnet mask is 22 bits long.

Question sources

Mock exam 4 · Question 8

Question 23 | Q00207

What is the special IP with all binary 1's used for?

A. A destination address to send to all devices on the same subnet

B. A destination address to send to all devices on another subnet

C. A destination address if a device is sending to itself

D. A source address when a device doesn't yet have an IP address

E. A source address if a device is sending to itself

Hint

Use the cited note definitions to identify the requested function or scope, then check each alternative against that same rule.

Answer A: Limited broadcast on the local subnet

All 32 one bits form 255.255.255.255, the limited-broadcast destination in NET23. Its scope is the local network; routers do not ordinarily forward it to another subnet. Self-reference uses loopback, while an unconfigured source can use 0.0.0.0. Thus the all-ones value is a destination broadcast, not either kind of source address.

Why each choice is right or wrong

A - Correct: The all-ones IPv4 address targets limited broadcast on the sender’s local network.

B - Incorrect: Limited broadcast is local in scope; it is not the destination for another subnet’s directed broadcast.

C - Incorrect: Sending to the host itself uses loopback, commonly 127.0.0.1, rather than the all-ones address.

D - Incorrect: An unconfigured source can use all-zero 0.0.0.0, not all-one 255.255.255.255.

E - Incorrect: The all-ones address is a broadcast destination, not a self-reference source address.

Primary note proof

Study-note section NET23

RFC1918 private blocks are 10.0.0.0/8, 172.16.0.0/12 (through 172.31.255.255), and 192.168.0.0/16. They can be reused internally but are not globally routed as public destinations. A LAN may also use legitimately assigned public addresses; private is common, not mandatory. 127.0.0.0/8 is IPv4 loopback, commonly 127.0.0.1, for local protocol access without an external link. 255.255.255.255 is limited broadcast; 0.0.0.0 can identify an unconfigured source. Link-local/APIPA uses 169.254.0.0/16, with edge /24 blocks excluded from normal automatic selection.

Study-note section NET11

Routers forward IP packets between networks using destination prefixes and next hops. They separate broadcast domains and normally do not forward local link broadcasts. A default gateway is usually a router, while a protocol gateway can translate application formats; therefore a gateway is not inherently a device that implements every OSI layer.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 19 | lines 2-22

Address Space: An address space is the total
number ofaddresses used by the protocol.
• If a protocol uses N bits to define an address,
the address space is 2N
because each bit can
have twodifferent values (0 or 1) and N bits
can have 2N values.
• IPv4 uses 32-bit addresses, which means that
the address space is 232 or 4,294,967,296
(more than 4billion).
Notations: There are two notations to show an IPv4 address:
• Binary notation: The IPv4 address is displayed
as 32bits. ex. 11000001 10000011 00011011
11111111
• Dotted decimal notation: To make the IPv4
address easier to read, Internet addresses are
usually written in decimal form with a decimal
point (dot) separatingthe bytes. Each byte (octet)
is 8 bits hence each number in dotted-decimal
notation is a value rangingfrom 0 to 255. Ex.
129.11.11.239

Data Communication and Computer Networking module | PDF page 19 | lines 23-36

Classful addressing : In classful addressing, the
addressspace is divided into five classes: A, B, C,
D, and E.
• Netid and Hostid In classful addressing, an IP

addressin class A, B, or C is divided into netid
and hostid.
Subnetting: It allows a network to be split into several
parts for internal use but still act like a single network to
the outsideworld.
• To implement subnetting, the router needs a
subnet mask that indicates the split between
network + subnet number and host. Ex.
255.255.252.0/22. A‖/22‖ to indicate that the
subnet mask is 22 bits long.

Question sources

Mock exam 4 · Question 9

Question 24 | Q00208

Which of the following technologies can allow a host with IP address 10.0.0.1 to access the internet?

A. NAT

B. Route import

C. Dynamic route

D. Static route

Hint

Separate address width, syntax, reserved scope and the supplied prefix or historical classful convention.

Answer A: NAT

The module prescribes translation of private internal addresses to a public address for Internet access. Conditional on the stem treating 10.0.0.1 as private, NAT is the offered mechanism. Evidence: PDF 19, 48, 19.

Why each choice is right or wrong

A - Correct: Private-to-public translation is exactly NAT (PDF 19, 48, 19.)

B - Incorrect: Importing routing information is not address translation (PDF 19, 48, 19.)

C - Incorrect: Dynamic path selection does not itself translate an internal address (PDF 19, 48, 19.)

D - Incorrect: Static routes do not themselves translate an internal address (PDF 19, 48, 19.)

Primary note proof

Study-note section NET29

A private host such as 10.0.0.1 commonly reaches the public Internet through NAT at a gateway, together with valid routing and a public external address. NAT alone does not supply a physical connection or DNS. A public address does not automatically grant permission to use it; both public and private unicast addresses can be used on a LAN under the correct allocation and subnet.

Study-note section NET30

Routing computes paths; forwarding chooses a next hop for an individual packet. Select the matching route with the longest prefix, then apply the routing system's tie-breaking criteria. A default /0 matches when nothing more specific does. Static routes are configured; dynamic protocols exchange reachability. Distance vector uses neighbor estimates, while link state distributes link information and computes shortest paths. Interior protocols operate within an autonomous system; BGP exchanges routes between systems.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 19 | lines 45-49

NAT (Network Address Translation): The scarcity of
network addresses in IPv4 led to the development of IPv6.
Due to this, we need to use private IP address inside the
organization and translate it to public IP address using
NAT.

Data Communication and Computer Networking module | PDF page 48 | lines 29-40

Network Address Translation (NAT)
NAT translates the IP addresses of computers in a local
network to a single IP address. This address is often used
by the router that connects the computers to the Internet.
The router can be connected to a DSL modem, cable
modem, T1 line, or even a dial-up modem. When other
computers on the Internet attempt to access computers
within the local network, they only see the IP address of
the router. This adds an extra level of security, since the
router can be configured as a firewall, only allowing
authorized systems to access the computers within the
network.

Data Communication and Computer Networking module | PDF page 19 | lines 52-64

ROUTING AND ROUTING PROTOCOLS
Routing is the act of moving information across an
internetwork from a source to a destination. At the heart of
such protocol is the routing algorithm that determines the
path for a packet.
• Routing requires a host or a router to have a
routingtable which is constructed by the routing
algorithm.

• There are wo kinds of routing algorithms (routing tables): nonadaptive (static) and adaptive (dynamic)
• And two kinds of protocols
o Interior routing protocols
o Exterior routing protocols

Question sources

Mock exam 4 · Question 10

Question 25 | Q00267

Which of the following protocol is used to define how messages are formatted and transmitted on the World Wide Web?

A. IP

B. FTP

C. SMTP

D. HTTP

Hint

Identify the requested service or delivery guarantee, then distinguish application roles, transport behavior and address configuration.

Answer D: HTTP

The question asks for the application protocol defining World Wide Web message exchange. HTTP defines web request/response semantics. IP supplies packet delivery beneath applications; FTP transfers files through its own protocol; SMTP submits and relays email. Those services do not define browser/server HTTP message formatting and exchange.

Why each choice is right or wrong

A - Incorrect: IP supplies best-effort packet delivery and does not define World Wide Web application-message semantics.

B - Incorrect: FTP is a file-transfer protocol with separate control and data connections, not the web-message protocol.

C - Incorrect: SMTP submits and relays mail rather than defining World Wide Web exchanges.

D - Correct: HTTP supplies web request/response semantics, matching the message formatting and transmission role asked about.

Primary note proof

Study-note section NET21

HTTP defines web request/response semantics; it is stateless, and a message body may be absent. HTTPS adds TLS protection. FTP transfers files using control and separate data connections; it is

not the same protocol as SFTP. SMTP submits and relays mail; POP3 retrieves messages and IMAP accesses/synchronizes server mailboxes. Saying SMTP handles both sending and end-user mailbox retrieval is inaccurate.

Study-note section NET16

IP supplies connectionless best-effort packet delivery, not end-to-end ordering or retransmission. IPv4 addresses are 32 bits. Its minimum header is 20 bytes and can grow to 60 bytes; it is not a 32-bit header. IHL counts 32-bit words; total length includes header and payload. TTL limits lifetime across routers; the protocol field identifies TCP, UDP or another upper-layer protocol.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 28 | lines 23-31

Telnet 23 SNMP 161
SMTP 25 TFTP 69
HTTP 80 DNS 53
FTP 21 POP3 110
DNS 53 DHCP 68
HTTPS 443 NTP 123
SSH 22 RPC 530
Table. Sample TCP and UDP port numbers from well-known category

Data Communication and Computer Networking module | PDF page 18 | lines 27-32

Application Layer
The Application Layer is a combination of Session, Presentation & Application Layers of OSI models and defines high level protocols like File Transfer (FTP), Electronic Mail (SMTP), Virtual Terminal (TELNET), Domain Name Service (DNS), etc.

Question sources

Mock exam 4 · Question 69

Question 26 | Q00347

What is the bit pattern for the first octet of a class -B network address?

A. 110XXXXX

B. 1110XXXXX

C. 10XXXXXX

D. 0XXXXXXX

Hint

Convert the mask to a prefix, separate network and host bits, and apply the relevant subnet-count or usable-host rule.

Answer C: 10XXXXXX

In historical classful IPv4 addressing, Class B starts with the two fixed bits 10; the remaining six bits of the first octet vary. This gives first-octet decimal values 128-191. The alternatives instead begin with the Class C, Class D and Class A patterns respectively; B also prints too many total bits for an octet.

Why each choice is right or wrong

A - Incorrect: The fixed prefix 110 identifies historical Class C rather than Class B.

B - Incorrect: The fixed prefix 1110 identifies multicast Class D; the printed pattern also exceeds eight positions.

C - Correct: Class B fixes the first two bits to 10 and permits six remaining first-octet bits.

D - Incorrect: A leading zero identifies historical Class A, not Class B.

Primary note proof

Study-note section NET22

> Historical classes use leading patterns: A 0 with /8, B 10 with /16, C 110 with /24; D 1110 is multicast and E 1111 reserved. Ordinary class-A first octets are 1-126 because 0 and 127 have special uses. B spans 128-191 and C 192-223. Default usable counts are 2^24-2, 2^16-2 and 254. Modern CIDR requires the actual prefix and overrides class defaults.

Study-note section NET22

> Write IPv4 as four decimal octets 0-255, or as 32 binary bits. Use weights 128,64,32,16,8,4,2,1 within each octet. Thus 11000001 10000011 00011011 11111111 is 193.131.27.255. A value such as 257 is impossible. Syntactic validity differs from assignability: an address ending .0 or .255 can be a host under some prefixes.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 19 | lines 23-36

> Classful addressing : In classful addressing, the
> addressspace is divided into five classes: A, B, C,
> D, and E.
> • Netid and Hostid In classful addressing, an IP
> addressin class A, B, or C is divided into netid
> and hostid.
> Subnetting: It allows a network to be split into several
> parts for internal use but still act like a single network to
> the outsideworld.
> • To implement subnetting, the router needs a

subnet mask that indicates the split between network + subnet number and host. Ex. 255.255.252.0/22. A‖/22‖ to indicate that the subnet mask is 22 bits long.

Question sources

Computer Science model exam · Question 78

University of Gondar model exam · Question 78

Question 27 | Q00348

Which OSI model layer is responsible for flow control?

A. Application Layer

B. Transport Layer

C. Session Layer

D. Presentation Layer

Hint

Match the requested scope or data unit to the layer duties in the note; distinguish hop delivery from end-to-end process delivery.

Answer B: Transport Layer

Among these four layers transport explicitly provides end-to-end flow control. Data link also provides flow control but is not offered. Evidence: PDF 16, 16, 16, 16.

Why each choice is right or wrong

A - Incorrect: Application provides access to resources (PDF 16, 16, 16, 16.)

B - Correct: Transport explicitly carries out flow control (PDF 16, 16, 16, 16.)

C - Incorrect: Session manages dialogs and checkpoints (PDF 16, 16, 16, 16.)

D - Incorrect: Presentation handles translation, compression and encryption (PDF 16, 16, 16, 16.)

Primary note proof

Study-note section NET17

TCP offers a reliable ordered byte stream using sequence numbers, acknowledgments, retransmission and windows. Flow control protects the receiver; congestion control protects network capacity. UDP sends independent datagrams with ports and a checksum but no built-in setup, delivery guarantee, retransmission or ordering. Live interactive traffic may choose UDP when late data is less useful than lost data. Application protocols can add reliability over UDP.

Study-note section NET19

OSI session roles establish/manage dialogs and can coordinate checkpoints so transfer resumes after interruption. Presentation roles translate encodings and handle compression/encryption. Compression reduces representation size; encryption hides content and need not shrink it. Application protocols provide services directly to applications. Practical implementations distribute these functions differently; TLS is not proof of a separate physical presentation-layer device.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 16 | lines 2-17

• At the sending side, the transport layer receives data from the session layer, divides it into units called segments and sends it to the network layer.
• To ensure process to process delivery the transport layer makes use of port address to identify the data from the sending and receiving process.
• The data can be transported in a connection oriented or connectionless manner.
• The Transport layer is responsible for segmentation and reassembly of the message into segments which bear sequence numbers.
• The transport layer also carries out flow control and error control functions; but unlike data link layer these are end to end rather than node to node.
• The main responsibility of the transport layer is process to process delivery of the entire message

Data Communication and Computer Networking module | PDF page 16 | lines 43-47

Application Layer
• The application layer enables the user to communicate its data to the receiver by providing certain services.
• The main Responsibility of Application layer is to provide the user access to network resources.

Data Communication and Computer Networking module | PDF page 16 | lines 18-32

Session Layer
• The session layer establishes a session between the communicating devices called dialog and synchronizes their interaction. It is the responsibility of the session layer to establish and synchronize the dialogs. It is also called the network dialog controller.
• The session layer at the sending side accepts data from the presentation layer adds checkpoints to it called sync bits and passes the data to the transport layer. At the receiving end the session layer receives

data from the transport layer removes the checkpoints inserted previously and passes the data to the presentation layer. So, the main responsibility of session layer is dialog control and synchronization.

Data Communication and Computer Networking module | PDF page 16 | lines 33-42

Presentation Layer
• The communicating devices may be having different platforms. The presentation layer performs translation, encryption and compression of data.
• The presentation layer receives the data from the application layer adds header which contains information related to encryption and compression and sends it to the session layer.
• So, the main responsibility of the Presentation layer is translation, compression and encryption.

Question sources

Computer Science model exam · Question 79

University of Gondar model exam · Question 79

Question 28 | Q00349

Which of the following networking device is used in physical layer?

A. Bridge

B. Router

C. Switch

D. Hub

Hint

Match the requested scope or data unit to the layer duties in the note; distinguish hop delivery from end-to-end process delivery.

Answer D: Hub

An active hub is a multiport repeater, and a repeater operates only at the physical layer. Evidence: PDF 12, 11, 12, 12, 12.

Why each choice is right or wrong

A - Incorrect: Bridge filters based on MAC (PDF 12, 11, 12, 12, 12.)

B - Incorrect: Router routes by IP (PDF 12, 11, 12, 12, 12.)

C - Incorrect: Switch filters/forwards by MAC (PDF 12, 11, 12, 12, 12.)

D - Correct: Active hub repeats physical signals (PDF 12, 11, 12, 12, 12.)

Primary note proof

Study-note section NET09

A repeater regenerates layer-1 signals without inspecting destination addresses. An active hub is a multiport repeater: it repeats incoming signals onto other ports, placing half-duplex endpoints in one collision domain. A passive hub is a connector. A hub neither learns MAC addresses nor eliminates collisions. An endpoint such as a network printer consumes services; routers, hubs and access points are intermediary devices.

Study-note section NET10

A bridge or ordinary Ethernet switch operates at layer 2. It learns source-MAC-to-port mappings, looks up the destination, forwards a known unicast to its port, filters it if the destination is on the incoming segment, and floods an unknown unicast or broadcast within its VLAN. A switch does not always send only to one destination port. Wireless access points normally bridge wireless and wired link-layer traffic.

Study-note section NET11

Routers forward IP packets between networks using destination prefixes and next hops. They separate broadcast domains and normally do not forward local link broadcasts. A default gateway is usually a router, while a protocol gateway can translate application formats; therefore a gateway is not inherently a device that implements every OSI layer.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 12 | lines 17-26

Active Hubs
An active hub is actually a multipart repeater. It is
normallyused to create connections between stations in
a physical startopology.
HUB: Hubs are commonly used to connect segments
(devices)of a LAN. Hubs don‘t filter information; instead
broadcast incoming packets to all computers connected to
it. A hub contains multiple ports which support 8, 12 or
24 RJ-45 ports. Two types: Passive hub and Active hub. It
is used in star or ring topology.

Data Communication and Computer Networking module | PDF page 11 | lines 54-55

Repeater: A repeater is a device that operates only in the physical
layer. A repeater receives a signal and, before it

Data Communication and Computer Networking module | PDF page 12 | lines 27-37

SWITCH: A switch filters and forwards data packets
across anetwork.
Unlike a hub which simply replicates what it receives on

oneport onto all the other ports, a switch keeps a record of the MAC addresses of the devices attached to it.
When the switch receives a data packet, it forwards the packetdirectly to the recipient device by looking up the MAC address.
• Switch is intelligent and expensive than Hub
• Switch is a point to point communication device
• Hub is a broadcasting device

Data Communication and Computer Networking module | PDF page 12 | lines 38-52

ROUTER: Router is a specialized network device used tointerconnect different types of network that uses different protocol.
Router allows the users to connect several LAN and WAN
• A LAN to another LAN
• A WAN to another WAN
• A LAN to the Internet
Routers use the routing table to determine how to forwardpackets.
• The list of routing tables provides directions to transfer the data to a particular network destination -various paths to forward the data.
• A router analyzes a destination IP address of a givenpacket and compares it with the routing table to decide the packet's next best path

Data Communication and Computer Networking module | PDF page 12 | lines 60-61

BRIDGE: Connects two LANS having the same protocol - (e.g. Ethernet or Token ring).

Question sources

Computer Science model exam · Question 80

University of Gondar model exam · Question 80

Question 29 | Q00350

Assuming that Company VWX has main site and remote site. The main site has three LANs with LAN 1 has 100 hosts, LAN 2 has 60 hosts, and LAN 3 has 29 hosts. The remote site has two LANs, each with 100 hosts. The network uses private addresses. The Internet service provider assigned the company the network 200.100.50.2/26.vThe remote site uses the network prefix 192.168.10.0/24. What subnets and masks can you use for the LANs at the remote site and conserve address space?

A. 192.168.10.0/25 and 192.168.10.128/25

B. 192.168.10.0/30 and 192.168.10.128/30

C. 192.168.10.64/26 and 192.168.10.192/26

D. 192.168.10.32/28 and 192.168.10.64/28

Hint

Convert the mask to a prefix, separate network and host bits, and apply the relevant subnet-count or usable-host rule.

Answer A: 192.168.10.0/25 and 192.168.10.128/25

Each remote LAN needs 100 hosts. /25 leaves seven bits (128 total addresses) and two nonoverlapping /25 blocks exactly partition the /24. A is the capacity-minimal offered division even without requiring a host-reservation formula. Evidence: PDF 19, 19.

Why each choice is right or wrong

A - Correct: 128 total per LAN can accommodate 100 and the blocks are disjoint (PDF 19, 19.)

B - Incorrect: Four total per /30 cannot hold 100 (PDF 19, 19.)

C - Incorrect: 64 total per /26 cannot hold 100 (PDF 19, 19.)

D - Incorrect: 16 total per /28 cannot hold 100 (PDF 19, 19.)

Primary note proof

Study-note section NET27

> For a /24 with LAN demands 100,60,29: allocate .0/25 (hosts .1-.126), .128/26 (.129-.190), and .192/27 (.193-.222); .224/27 remains. Two remote LANs of 100 each fit .0/25 and .128/25 within a separate /24. Count router interfaces as hosts if not already included in the demand.

Study-note section NET26

> For H hosts, choose the smallest h satisfying 2^h-2≥H, then p=32-h. For 24 hosts use /27; 52 or 57 use /26; 100 use /25; 500 use /23. For at least six equal subnets choose b=3. A Class C /24 split to /27 yields eight subnets. Always check both the number of subnets and the host capacity.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 19 | lines 2-22

Address Space: An address space is the total number ofaddresses used by the protocol.
• If a protocol uses N bits to define an address, the address space is 2N because each bit can have twodifferent values (0 or 1) and N bits can have 2N values.
• IPv4 uses 32-bit addresses, which means that the address space is 232 or 4,294,967,296 (more than 4billion).
Notations: There are two notations to show an IPv4 address:
• Binary notation: The IPv4 address is displayed as 32bits. ex. 11000001 10000011 00011011 11111111
• Dotted decimal notation: To make the IPv4 address easier to read, Internet addresses are usually written in decimal form with a decimal point (dot) separatingthe bytes. Each byte (octet) is 8 bits hence each number in dotted-decimal notation is a value rangingfrom 0 to 255. Ex. 129.11.11.239

Data Communication and Computer Networking module | PDF page 19 | lines 23-36

Classful addressing : In classful addressing, the addressspace is divided into five classes: A, B, C, D, and E.
• Netid and Hostid In classful addressing, an IP addressin class A, B, or C is divided into netid and hostid.
Subnetting: It allows a network to be split into several parts for internal use but still act like a single network to the outsideworld.
• To implement subnetting, the router needs a subnet mask that indicates the split between network + subnet number and host. Ex. 255.255.252.0/22. A‖/22‖ to indicate that the subnet mask is 22 bits long.

Question sources

Computer Science model exam · Question 81

University of Gondar model exam · Question 81

Question 30 | Q00351

The main site uses the network prefix 192.168.15.0/24. What subnets and masks can you use to provide sufficient addresses for LANs at the main site and conserve address space?

A. 192.168.15.0/25 for LAN 1, 192.168.15.128/26 for LAN 2, and 192.168.15.192/27 for LAN

B. 192.168.15.0/26 for LAN 1, 192.168.15.128/26 for LAN 2, and 172.15.192.0/29 for LAN 3

C. 192.168.15.0/27 for LAN 1, 192.168.15.128/26 for LAN 2, and 172.15.192.0/25 for LAN 3

D. 192.168.15.0/100 for LAN 1, 192.168.15.128/60 for LAN 2, and 172.15.192.0/29 for LAN 3

Hint

Convert the mask to a prefix, separate network and host bits, and apply the relevant subnet-count or usable-host rule.

Answer A: 192.168.15.0/25 for LAN 1, 192.168.15.128/26 for LAN 2, and 192.168.15.192/27 for LAN

With Q29 context (100,60,29 hosts), A allocates 128,64,32 total addresses without overlap within 192.168.15.0/24. These are the smallest offered powers of two meeting the host counts; other choices fail total capacity, prefix syntax or membership. Evidence: PDF 19, 19.

Why each choice is right or wrong

A - Correct: The /25,/26,/27 division is sufficient and stays within the parent (PDF 19, 19.)

B - Incorrect: First /26 has only 64 total addresses for 100 hosts; third block is outside the parent (PDF 19, 19.)

C - Incorrect: First /27 has only 32 total for 100; third block is outside the parent (PDF 19, 19.)

D - Incorrect: /100 and /60 exceed the 32-bit IPv4 width; third block is outside the parent (PDF 19, 19.)

Primary note proof

Study-note section NET27

> VLSM assigns different masks to different LAN sizes. Sort demands largest first, round each to a power-of-two address block including reservations, allocate aligned nonoverlapping blocks within the parent, and leave the remaining space explicit.

Study-note section NET27

> For a /24 with LAN demands 100,60,29: allocate .0/25 (hosts .1-.126), .128/26 (.129-.190), and .192/27 (.193-.222); .224/27 remains. Two remote LANs of 100 each fit .0/25 and .128/25 within a separate /24. Count router interfaces as hosts if not already included in the demand.

Study-note section NET25

> For ordinary broadcast LANs let h=32-p. Total addresses=2^h; usable hosts=2^h-2, reserving network and directed broadcast. Find the changing octet's increment as 256-mask octet, round the address down to a multiple, and extend through the next boundary minus one.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 19 | lines 2-22

Address Space: An address space is the total
number ofaddresses used by the protocol.
• If a protocol uses N bits to define an address,
the address space is 2N
because each bit can
have twodifferent values (0 or 1) and N bits
can have 2N values.
• IPv4 uses 32-bit addresses, which means that
the address space is 232 or 4,294,967,296
(more than 4billion).
Notations: There are two notations to show an IPv4 address:
• Binary notation: The IPv4 address is displayed
as 32bits. ex. 11000001 10000011 00011011
11111111
• Dotted decimal notation: To make the IPv4
address easier to read, Internet addresses are
usually written in decimal form with a decimal
point (dot) separatingthe bytes. Each byte (octet)
is 8 bits hence each number in dotted-decimal
notation is a value rangingfrom 0 to 255. Ex.
129.11.11.239

Data Communication and Computer Networking module | PDF page 19 | lines 23-36

Classful addressing : In classful addressing, the
addressspace is divided into five classes: A, B, C,
D, and E.
• Netid and Hostid In classful addressing, an IP
addressin class A, B, or C is divided into netid
and hostid.
Subnetting: It allows a network to be split into several
parts for internal use but still act like a single network to
the outsideworld.
• To implement subnetting, the router needs a
subnet mask that indicates the split between
network + subnet number and host. Ex.
255.255.252.0/22. A‖/22‖ to indicate that the
subnet mask is 22 bits long.

Question sources

Computer Science model exam · Question 82

University of Gondar model exam · Question 82

Question 31 | Q00352

Which network and mask would you use for the WAN link to save the most address space?

A. 192.168.11.240/27

B. 192.168.11.240/28

C. 192.168.11.240/29

D. 192.168.11.240/30

Hint

Use the cited note definitions to identify the requested function or scope, then check each alternative against that same rule.

Answer D: 192.168.11.240/30

Of the offered prefixes, /30 leaves the fewest host bits: two, giving four total addresses. It therefore consumes the least address space for a two-endpoint WAN under the conventional allocation implied by the options. Evidence: PDF 19, 19.

Why each choice is right or wrong

A - Incorrect: /27 consumes 32 addresses; .240 is also unaligned as a /27 network (PDF 19, 19.)

B - Incorrect: /28 consumes 16 addresses (PDF 19, 19.)

C - Incorrect: /29 consumes eight addresses (PDF 19, 19.)

D - Correct: /30 consumes four addresses and .240 is aligned (PDF 19, 19.)

Primary note proof

Study-note section NET28

> A conventional /30 has four addresses and two usable endpoints; check the link and addressing assumptions when selecting a WAN prefix. RFC3021 permits /31 on supported point-to-point links: both addresses are endpoints, so the subtract-two rule does not apply. /32 identifies one address/host route. Do not claim /30 is universally the smallest valid link prefix.

Study-note section NET25

> For ordinary broadcast LANs let h=32-p. Total addresses=2^h; usable hosts=2^h-2, reserving network and directed broadcast. Find the changing octet's increment as 256-mask octet, round the address down to a multiple, and extend through the next boundary minus one.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 19 | lines 2-22

> Address Space: An address space is the total
> number ofaddresses used by the protocol.
> • If a protocol uses N bits to define an address,
> the address space is 2N

because each bit can
have twodifferent values (0 or 1) and N bits
can have 2N values.
• IPv4 uses 32-bit addresses, which means that
the address space is 232 or 4,294,967,296
(more than 4billion).
Notations: There are two notations to show an IPv4 address:
• Binary notation: The IPv4 address is displayed
as 32bits. ex. 11000001 10000011 00011011
11111111
• Dotted decimal notation: To make the IPv4
address easier to read, Internet addresses are
usually written in decimal form with a decimal
point (dot) separatingthe bytes. Each byte (octet)
is 8 bits hence each number in dotted-decimal
notation is a value rangingfrom 0 to 255. Ex.
129.11.11.239

Data Communication and Computer Networking module | PDF page 19 | lines 23-36

Classful addressing : In classful addressing, the
addressspace is divided into five classes: A, B, C,
D, and E.
• Netid and Hostid In classful addressing, an IP
addressin class A, B, or C is divided into netid
and hostid.
Subnetting: It allows a network to be split into several
parts for internal use but still act like a single network to
the outsideworld.
• To implement subnetting, the router needs a
subnet mask that indicates the split between
network + subnet number and host. Ex.
255.255.252.0/22. A‖/22‖ to indicate that the
subnet mask is 22 bits long.

Question sources

Computer Science model exam · Question 83

University of Gondar model exam · Question 89

Question 32 | Q00535

Among the following one helps to resolve internet name into IP Address.

A. Domain Name System

B. Address Resolution Protocol

C. User Datagram Protocol

D. Transmission Control Protocol

Hint

Separate address width, syntax, reserved scope and the supplied prefix or historical classful convention.

Answer A: Domain Name System

DNS provides external naming in contrast to locally stored addresses. ARP instead resolves an already-known IP to a hardware address. Evidence: PDF 18, 65, 17, 18.

Why each choice is right or wrong

A - Correct: Domain Name Service is the naming mechanism (PDF 18, 65, 17, 18.)

B - Incorrect: ARP maps IP to physical address, not domain to IP (PDF 18, 65, 17, 18.)

C - Incorrect: UDP provides process delivery (PDF 18, 65, 17, 18.)

D - Incorrect: TCP provides reliable connection-oriented process delivery (PDF 18, 65, 17, 18.)

Primary note proof

Study-note section NET20

> DNS resolves names to records, including IPv4 A and IPv6 AAAA addresses; it can use UDP or TCP port 53. DHCP dynamically leases IPv4 settings, commonly address, mask, gateway and DNS server. Its basic exchange is discover, offer, request, acknowledge. IP itself does not assign addresses.

Study-note section NET20

> ARP resolves an on-link IPv4 next hop to a link address, using a broadcast request and normally unicast reply. For an off-subnet target, ARP resolves the gateway, not the remote target’s MAC. It bridges the network/link addressing boundary and is often classified at the link layer; calling ARP simply a network protocol uses a loose textbook convention. RARP reverses hardware-to-IP lookup; BOOTP/DHCP support boot configuration. ICMP reports errors and diagnostics; IGMP manages IPv4 multicast membership. These are separate companion protocols, not four pieces whose combination is IP.

Study-note section NET17

> TCP offers a reliable ordered byte stream using sequence numbers, acknowledgments, retransmission and windows. Flow control protects the receiver; congestion control protects network capacity. UDP sends independent datagrams with ports and a checksum but no built-in

setup, delivery guarantee, retransmission or ordering. Live interactive traffic may choose UDP when late data is less useful than lost data. Application protocols can add reliability over UDP.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 18 | lines 27-32

Application Layer
The Application Layer is a combination of Session,
Presentation & Application Layers of OSI models and defines
high level protocols like File Transfer (FTP), Electronic Mail
(SMTP), Virtual Terminal (TELNET), Domain Name Service
(DNS), etc.

Data Communication and Computer Networking module | PDF page 65 | lines 31-38

/etc/hosts
The /etc/hosts file always contains the localhost IP
address, 127.0.0.1, which is
usedfor interprocess communication.
Never remove this line! Sometimes contains
addresses of additional hosts, whichcan be contacted
without using an external naming service such as
DNS (the Domain Name Server).

Data Communication and Computer Networking module | PDF page 17 | lines 44-53

ARP - Address Resolution Protocol: It is used to
resolve thephysical address of a device on a network,
where its logical address is known.
Physical address is the 48 bit address that is imprinted
on theNIC or LAN card, Logical address is the Internet
Address orcommonly known as IP address that is used
to uniquely & universally identify a device.
RARP- Reverse Address Resolution Protocol: It is
used bya device on the network to find its Internet
address when it knows its physical address.

Data Communication and Computer Networking module | PDF page 18 | lines 9-21

TCP - Transmission Control Protocol: TCP is a reliable
connection-oriented, reliable protocol. i.e. a connection is
established between the sender and receiver before the data can
be transmitted. It divides the data it receives from the upper
layer into segments and tags a sequence number to each
segment which is used at the receiving end for reordering of
data.
UDP - User Datagram Protocol: UDP is a simple protocol
used for process to process transmission. It is an unreliable,
connectionless protocol for applications that do not require flow

control or error control. It simply adds port address, checksum and length information to the data it receives from the upper layer.

Question sources

Computer Science model exam · 2015 · Question 4

Question 33 | Q00536

You have been asked to create a subnet that supports 24 hosts. What subnet mask you use?

A. 255.255.255.224

B. 255.255.255.248

C. 255.255.255.240

D. 255.255.255.252

Hint

Convert the mask to a prefix, separate network and host bits, and apply the relevant subnet-count or usable-host rule.

Answer A: 255.255.255.224

A /27 mask (224=11100000) leaves five bits, giving 32 total addresses, enough for 24 hosts. All other options have fewer than 24 total addresses, so reservations do not affect the selection. Evidence: PDF 19, 19.

Why each choice is right or wrong

A - Correct: 224 leaves five bits and 32 addresses (PDF 19, 19.)

B - Incorrect: 248 leaves three bits and eight addresses (PDF 19, 19.)

C - Incorrect: 240 leaves four bits and 16 addresses (PDF 19, 19.)

D - Incorrect: 252 leaves two bits and four addresses (PDF 19, 19.)

Primary note proof

Study-note section NET26

For H hosts, choose the smallest h satisfying 2^h-2≥H, then p=32-h. For 24 hosts use /27; 52 or 57 use /26; 100 use /25; 500 use /23. For at least six equal subnets choose b=3. A Class C /24 split to /27 yields eight subnets. Always check both the number of subnets and the host capacity.

Study-note section NET24

A /p IPv4 prefix has p leading one bits followed by 32-p zeros. Partial octet masks are 128,192,224,240,248,252,254. /19 is 255.255.224.0; /20 is 255.255.240.0; /21 is 255.255.248.0, correcting the study guide’s 255.248.0.0 mistake.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 19 | lines 2-22

Address Space: An address space is the total
number ofaddresses used by the protocol.
• If a protocol uses N bits to define an address,
the address space is 2N
because each bit can
have twodifferent values (0 or 1) and N bits
can have 2N values.
• IPv4 uses 32-bit addresses, which means that
the address space is 232 or 4,294,967,296
(more than 4billion).
Notations: There are two notations to show an IPv4 address:
• Binary notation: The IPv4 address is displayed
as 32bits. ex. 11000001 10000011 00011011
11111111
• Dotted decimal notation: To make the IPv4
address easier to read, Internet addresses are
usually written in decimal form with a decimal
point (dot) separatingthe bytes. Each byte (octet)
is 8 bits hence each number in dotted-decimal
notation is a value rangingfrom 0 to 255. Ex.
129.11.11.239

Data Communication and Computer Networking module | PDF page 19 | lines 23-36

Classful addressing : In classful addressing, the
addressspace is divided into five classes: A, B, C,
D, and E.
• Netid and Hostid In classful addressing, an IP
addressin class A, B, or C is divided into netid
and hostid.
Subnetting: It allows a network to be split into several
parts for internal use but still act like a single network to
the outsideworld.
• To implement subnetting, the router needs a
subnet mask that indicates the split between
network + subnet number and host. Ex.
255.255.252.0/22. A‖/22‖ to indicate that the
subnet mask is 22 bits long.

Question sources

Computer Science model exam · 2015 · Question 5

Question 34 | Q00538

Assume you are asking to establish a network using 50(fifty) computers in mesh topology. How many cables required to establish a network?

A. 2225

B. 1225

C. 1450

D. 2450

Hint

Draw the links and identify shared components, alternate paths and the effect of the specified failure or growth requirement.

Answer B: 1225

Full-mesh cable count is n(n-1)/2, so 50×49/2=1225 distinct undirected cables. Each cable serves a pair and must not be counted twice. Evidence: PDF 23.

Why each choice is right or wrong

A - Incorrect: 2225 is not 50×49/2 (PDF 23.)

B - Correct: 1225 is the computed cable count (PDF 23.)

C - Incorrect: 1450 is not the pair count (PDF 23.)

D - Incorrect: 2450 counts both directions of each cable (PDF 23.)

Primary note proof

Study-note section NET08

> A full undirected mesh of n nodes needs n(n-1)/2 links and n-1 interfaces per node. For 50 nodes: 50×49/2=1225 links. Redundant paths improve fault tolerance at greater cable and interface cost.

Study-note section NET08

> Physical topology describes link layout; logical topology describes communication/access relationships. Point-to-point links join two endpoints; multipoint links share a medium. A full mesh consists of point-to-point links.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 23 | lines 45-53

> Mesh Topology: in this topology devices are
> connected with many redundant interconnections
> between network nodes. In a full mesh topology,
> every node has a connection to every other node in
> the network, which makes it the most expensive
> topology over all the other topologies. The number of

cables grows fast as the number of nodes increases,
and it can be calculated by using the general formula
((n (n - 1)) /2), where n is the number of nodes in the

Question sources

Computer Science model exam · 2015 · Question 7

Question 35 | Q00552

A TCP/IP protocol for mapping an Internet Protocol address (IP address) to a physical machine address (MAC) that is recognized in the local network.

A. Address Resolution Protocol

B. Domain Name System

C. Revers Address Resolution Protocol

D. Internet Control Messaging Protocol

Hint

Identify the requested service or delivery guarantee, then distinguish application roles, transport behavior and address configuration.

Answer A: Address Resolution Protocol

The known IP to MAC direction is explicitly ARP. Reverse ARP uses the opposite known and unknown addresses. Evidence: PDF 17, 18, 17.

Why each choice is right or wrong

A - Correct: ARP resolves physical from logical address (PDF 17, 18, 17.)

B - Incorrect: DNS is a name service, not IP-to-MAC resolution (PDF 17, 18, 17.)

C - Incorrect: RARP finds Internet address from physical address (PDF 17, 18, 17.)

D - Incorrect: ICMP signals transit problems (PDF 17, 18, 17.)

Primary note proof

Study-note section NET20

ARP resolves an on-link IPv4 next hop to a link address, using a broadcast request and normally unicast reply. For an off-subnet target, ARP resolves the gateway, not the remote target’s MAC. It bridges the network/link addressing boundary and is often classified at the link layer; calling ARP simply a network protocol uses a loose textbook convention. RARP reverses hardware-to-IP lookup; BOOTP/DHCP support boot configuration. ICMP reports errors and diagnostics; IGMP manages IPv4 multicast membership. These are separate companion protocols, not four pieces whose combination is IP.

Study-note section NET20

DNS resolves names to records, including IPv4 A and IPv6 AAAA addresses; it can use UDP or TCP port 53. DHCP dynamically leases IPv4 settings, commonly address, mask, gateway and DNS server. Its basic exchange is discover, offer, request, acknowledge. IP itself does not assign addresses.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 17 | lines 44-53

ARP - Address Resolution Protocol: It is used to
resolve thephysical address of a device on a network,
where its logical address is known.
Physical address is the 48 bit address that is imprinted
on theNIC or LAN card, Logical address is the Internet
Address orcommonly known as IP address that is used
to uniquely & universally identify a device.
RARP- Reverse Address Resolution Protocol: It is
used bya device on the network to find its Internet
address when it knows its physical address.

Data Communication and Computer Networking module | PDF page 18 | lines 27-32

Application Layer
The Application Layer is a combination of Session,
Presentation & Application Layers of OSI models and defines
high level protocols like File Transfer (FTP), Electronic Mail
(SMTP), Virtual Terminal (TELNET), Domain Name Service
(DNS), etc.

Data Communication and Computer Networking module | PDF page 17 | lines 54-59

ICMP- Internet Control Message Protocol: It is a
signaling mechanism used to inform the sender about
datagram problemsthat occur during transit. It is used by
intermediate devices.
IGMP- Internet Group Message Protocol: It is a mechanism
that allows sending the same message to a group of recipients.

Question sources

Computer Science model exam · 2015 · Question 21

Question 36 | Q00553

One of the following is false the characteristics of controlled access in datalink layer.

A. Only one station is transmit at a time.

B. There will be a chance of collision.

C. Devices wishing to transmit must wait their turn.

D. Some deterministic networks use token passing.

Hint

Match the requested scope or data unit to the layer duties in the note; distinguish hop delivery from end-to-end process delivery.

Answer B: There will be a chance of collision.

The module characterizes controlled access as permission-based and describes the medium-control objective as preventing simultaneous speakers. Thus the collision-chance characterization conflicts with its ideal controlled-access model. Evidence: PDF 21.

Why each choice is right or wrong

A - Incorrect: One transmitter at a time matches controlled permission (PDF 21.)

B - Correct: Colliding simultaneous access is inconsistent with the described controlled-access rule (PDF 21.)

C - Incorrect: Waiting for permission follows get permission (PDF 21.)

D - Incorrect: Token passing is explicitly in controlled access (PDF 21.)

Primary note proof

Study-note section NET14

> Controlled access uses polling, reservations or a token to grant turns; correctly coordinated access avoids contention collisions. Channelization divides frequency, time or code resources. Stop-and-wait sends one frame and waits for ACK, retransmitting on timeout; sequence bits distinguish duplicates. Sliding windows permit multiple unacknowledged frames. Link reliability/flow control is hop-local; transport reliability/flow control is end-to-end. Ethernet detects corruption but does not itself guarantee reliable delivery.

Study-note section NET14

> Random access allows contention: ALOHA sends opportunistically; CSMA senses before sending. In legacy half-duplex Ethernet, CSMA/CD detects collision, sends a jam indication, stops, and retries after random backoff. The jam signals a collision, not its clearance. Wi-Fi 802.11 uses CSMA/CA with waiting/backoff and acknowledgments; sensing does not eliminate hidden-terminal collisions.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 21 | lines 6-26

MEDIUM ACCESS CONTROL
The problem of controlling the access to the medium is similarto the rules of speaking in a meeting (the right to speak isupheld; two people do not speak at the same time; do notinterrupt each other; do not monopolize the discussion; ...) Three categories of multiple access protocols
Random Access Protocols - try your best like taxis do
• MA - Multiple Access
• CSMA - Carrier Sense MA
• CSMA/CD - CSMA with Collision Detection
• CSMA/CA - CSMA with Collision AvoidanceControlled-Access Protocols - get permission
• Reservation
• Polling
• Token Passing
Channelization Protocols - simultaneous use
• FDMA - Frequency-Division MA
• TDMA - Time-Division MA
• CDMA - Code-Division MA

Question sources

Computer Science model exam · 2015 · Question 22

Question 37 | Q00559

Among the following well known port number of TCP the port number of HTTP is:

A. 80

B. 25

C. 21

D. 110

Hint

Identify the requested service or delivery guarantee, then distinguish application roles, transport behavior and address configuration.

Answer A: 80

The module port table pairs HTTP with TCP port 80. Evidence: PDF 28.

Why each choice is right or wrong

A - Correct: 80 is paired with HTTP (PDF 28.)

B - Incorrect: 25 is SMTP (PDF 28.)

C - Incorrect: 21 is FTP (PDF 28.)

D - Incorrect: 110 is POP3 (PDF 28.)

Primary note proof

Study-note section NET21

> Usual service ports: FTP control 21, SSH 22, Telnet 23, SMTP relay 25, DNS 53, HTTP 80, POP3 110, IMAP 143, HTTPS 443. Telnet provides unencrypted remote terminals; SSH protects remote access. Servers can be configured on other ports. A browser's HTTP exchange does not determine the physical duplex mode of its network interface.

Study-note section NET17

> Ports identify transport endpoints; the application can choose a transport and request socket buffer sizes, subject to OS limits. A TCP connection is identified by source/destination IP and source/destination port, with TCP understood. IPv4 protocol numbers identify upper protocols; 80 is a usual HTTP port, not an IP protocol number. Clients often use ephemeral ports. SCTP is a reliable message-oriented transport with multiple streams.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 28 | lines 23-31

> Telnet 23 SNMP 161
> SMTP 25 TFTP 69
> HTTP 80 DNS 53
> FTP 21 POP3 110
> DNS 53 DHCP 68
> HTTPS 443 NTP 123
> SSH 22 RPC 530
> Table. Sample TCP and UDP port numbers from well-
> known category

Question sources

Computer Science model exam · 2015 · Question 28

Question 38 | Q00560

Which organizational networking term describes exposing selected internal services to approved users outside the organization?

A. Internet

B. Extranet

C. intranet

D. All

Hint

Match the requested scope or data unit to the layer duties in the note; distinguish hop delivery from end-to-end process delivery.

Answer B: Extranet

Access scope determines the answer: an extranet extends selected organizational services to approved outsiders. An intranet serves members internally, while the Internet is the global network of networks. Neither organizational term determines geographic size or requires a particular physical connection. The question therefore asks about controlled external access rather than treating every external link as the same network category.

Why each choice is right or wrong

A - Incorrect: The Internet is the global network of networks; it does not specifically name controlled access to an organization’s selected services.

B - Correct: An extranet exposes selected services to approved outsiders.

C - Incorrect: An intranet describes internal organizational access.

D - Incorrect: The three terms have different scopes, so all is not the requested category.

Primary note proof

Study-note section NET02

> An intranet serves an organization internally; an extranet exposes selected services to approved outsiders. Neither term alone specifies geographic size. A client requests a service; a server supplies it. Peer systems may perform both roles. Dedicated servers concentrate on service workloads but can still be clients of DNS, backup or update services. A ten-user cutoff is a teaching guideline, not a technical law. Centralization simplifies administration but creates dependencies; peer networks still need security.

Study-note section NET02

> PAN connects personal devices, such as Bluetooth accessories. LAN covers a local building or campus; MAN spans a metropolitan region; WAN connects distant regions. Device count alone does not determine the category. The Internet is a global network of networks, commonly the largest example of a WAN.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 22 | lines 2-19

> A network can be defined as two or more computers
> connected together in such a way that they can share
> resources. The primary purpose of a network is to share
> resources, and a resource could be:
> • a file,
> • a folder,
> • a printer,

• a disk drive, or just about anything else that exists on a computer.
Therefore, a computer network is simply a collection of computers or other hardware devices that are connected together, either physically or logically, using special hardware and software, to allow them to exchange information and cooperate. Networking is the term that describes the processes involved in designing, implementing, upgrading, managing and otherwise working with networks and network technologies.

Data Communication and Computer Networking module | PDF page 24 | lines 23-35

Network Architecture: based on the architecture (where do the clients get the shared resources?), networks can be categorized into three:
Client-Server Architecture: There can be one or more systems acting as Server. Other being Client, request the Server to serve requests. Servers take and process request on clients' behalf.
Peer-to-Peer (Point-to-point): Two systems can be connected Point-to-Point, or in other words back-to-back fashion. They both reside on same level and called peers.
There can be hybrid network which involves network architecture of both the above types.

Question sources

Computer Science model exam · 2015 · Question 29

Question 39 | Q00564

Class B private IP address space ranges:

A. 10.0.0.0----------19.255.255.255

B. 128.12.0.0--------191.24.255.255

C. 172.16.0.0--------172.31.255.255

D. 192.168.0.0------192.168.255.255

Hint

Separate address width, syntax, reserved scope and the supplied prefix or historical classful convention.

Answer C: 172.16.0.0 through 172.31.255.255

The private allocation within the historical Class B range is 172.16.0.0/12. Its twelve fixed bits leave first octet 172 and second octets 16-31, inclusive. The 192.168 range is also private but lies in historical Class C space; the other printed ranges are not RFC1918 private allocations.

Why each choice is right or wrong

A - Incorrect: The private 10/8 block ends at 10.255.255.255; extending it through first octet 19 includes public space.

B - Incorrect: This broad portion of historical Class B space is not a designated RFC1918 private allocation.

C - Correct: The 172.16/12 private block spans exactly 172.16.0.0 through 172.31.255.255.

D - Incorrect: 192.168/16 is private, but it lies in historical Class C space rather than Class B.

Primary note proof

Study-note section NET23

> RFC1918 private blocks are 10.0.0.0/8, 172.16.0.0/12 (through 172.31.255.255), and 192.168.0.0/16. They can be reused internally but are not globally routed as public destinations. A LAN may also use legitimately assigned public addresses; private is common, not mandatory. 127.0.0.0/8 is IPv4 loopback, commonly 127.0.0.1, for local protocol access without an external link. 255.255.255.255 is limited broadcast; 0.0.0.0 can identify an unconfigured source. Link-local/APIPA uses 169.254.0.0/16, with edge /24 blocks excluded from normal automatic selection.

Study-note section NET22

> Historical classes use leading patterns: A 0 with /8, B 10 with /16, C 110 with /24; D 1110 is multicast and E 1111 reserved. Ordinary class-A first octets are 1-126 because 0 and 127 have special uses. B spans 128-191 and C 192-223. Default usable counts are 2^24-2, 2^16-2 and 254. Modern CIDR requires the actual prefix and overrides class defaults.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 19 | lines 23-36

> Classful addressing : In classful addressing, the
> addressspace is divided into five classes: A, B, C,
> D, and E.
> • Netid and Hostid In classful addressing, an IP
> addressin class A, B, or C is divided into netid
> and hostid.
> Subnetting: It allows a network to be split into several
> parts for internal use but still act like a single network to
> the outsideworld.
> • To implement subnetting, the router needs a
> subnet mask that indicates the split between
> network + subnet number and host. Ex.

255.255.252.0/22. A‖/22‖ to indicate that the subnet mask is 22 bits long.

Data Communication and Computer Networking module | PDF page 19 | lines 45-49

NAT (Network Address Translation): The scarcity of network addresses in IPv4 led to the development of IPv6. Due to this, we need to use private IP address inside the organization and translate it to public IP address using NAT.

Question sources

Computer Science model exam · 2015 · Question 33

Question 40 | Q00570

Among the protocol one is used to provide remote access to servers and networking devices.

A. HTTP

B. SMTP

C. Telnet (terminal emulation protocol)

D. FTP

Hint

Compare signal repetition, frame forwarding, packet routing and policy enforcement using the stated device or traffic assumptions.

Answer C: Telnet (terminal emulation protocol)

TELNET is explicitly the Virtual Terminal protocol, which fits terminal emulation for remote access to servers or devices. Evidence: PDF 18.

Why each choice is right or wrong

A - Incorrect: HTTP is not the listed virtual-terminal service (PDF 18.)

B - Incorrect: SMTP is electronic mail (PDF 18.)

C - Correct: TELNET is explicitly virtual terminal (PDF 18.)

D - Incorrect: FTP is file transfer (PDF 18.)

Primary note proof

Study-note section NET21

Usual service ports: FTP control 21, SSH 22, Telnet 23, SMTP relay 25, DNS 53, HTTP 80, POP3 110, IMAP 143, HTTPS 443. Telnet provides unencrypted remote terminals; SSH protects remote access. Servers can be configured on other ports. A browser's HTTP exchange does not determine the physical duplex mode of its network interface.

Study-note section NET21

HTTP defines web request/response semantics; it is stateless, and a message body may be absent. HTTPS adds TLS protection. FTP transfers files using control and separate data connections; it is not the same protocol as SFTP. SMTP submits and relays mail; POP3 retrieves messages and IMAP accesses/synchronizes server mailboxes. Saying SMTP handles both sending and end-user mailbox retrieval is inaccurate.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 18 | lines 27-32

Application Layer
The Application Layer is a combination of Session,
Presentation & Application Layers of OSI models and defines
high level protocols like File Transfer (FTP), Electronic Mail
(SMTP), Virtual Terminal (TELNET), Domain Name Service
(DNS), etc.

Question sources

Computer Science model exam · 2015 · Question 39

Question 41 | Q00574

The function of protocols in transport layer (TCP and UDP) includes following except,

A. Segment upper-layer application data.

B. Establish end-to-end operations.

C. Provide flow control

D. Addressing packets

Hint

Match the requested scope or data unit to the layer duties in the note; distinguish hop delivery from end-to-end process delivery.

Answer D: Addressing packets

Transport segments upper data, provides end-to-end process operations, and may provide flow control through TCP. Logical packet addressing belongs to network delivery. Not every UDP operation provides flow control.

Why each choice is right or wrong

A - Incorrect: Segmentation is explicit transport work

B - Incorrect: Process-to-process delivery is end-to-end

C - Incorrect: Flow control is supported by the transport layer, though not UDP

D - Correct: IP packet addressing is assigned to the network layer

Primary note proof

Study-note section NET17

TCP offers a reliable ordered byte stream using sequence numbers, acknowledgments, retransmission and windows. Flow control protects the receiver; congestion control protects network capacity. UDP sends independent datagrams with ports and a checksum but no built-in setup, delivery guarantee, retransmission or ordering. Live interactive traffic may choose UDP when late data is less useful than lost data. Application protocols can add reliability over UDP.

Study-note section NET16

IP supplies connectionless best-effort packet delivery, not end-to-end ordering or retransmission. IPv4 addresses are 32 bits. Its minimum header is 20 bytes and can grow to 60 bytes; it is not a 32-bit header. IHL counts 32-bit words; total length includes header and payload. TTL limits lifetime across routers; the protocol field identifies TCP, UDP or another upper-layer protocol.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 16 | lines 2-17

• At the sending side, the transport layer receives data from the session layer, divides it into units called segments and sends it to the network layer.
• To ensure process to process delivery the transport layer makes use of port address to identify the data from the sending and receiving process.
• The data can be transported in a connection oriented or connectionless manner.
• The Transport layer is responsible for segmentation and reassembly of the message into segments which bear sequence numbers.
• The transport layer also carries out flow control and error control functions; but unlike data link layer these are end to end rather than node to node.
• The main responsibility of the transport layer is process to process delivery of the entire message

Data Communication and Computer Networking module | PDF page 15 | lines 41-61

Network Layer
• The network layer makes sure that the data is deliveredto the receiver despite multiple intermediate devices.
• The network layer at the sending side accepts data from the transport layer, divides it into packets, addsaddressing information in the header and passes it tothe data link layer.

• The network layer is responsible for source todestination of delivery of data.
• The network layer uses logical address commonlyknown as IP address to recognize devices on the network.
• Each packet is independent of the other and may travelusing different routes to reach the receiver hence may arrive out of turn at the receiver (Routing).
• The Network layer does not perform any flow controlor error control
• The main responsibility of Network Layer is transmission of packets from source to destination

Data Communication and Computer Networking module | PDF page 18 | lines 9-21

TCP - Transmission Control Protocol: TCP is a reliable connection-oriented, reliable protocol. i.e. a connection is established between the sender and receiver before the data can be transmitted. It divides the data it receives from the upper layer into segments and tags a sequence number to each segment which is used at the receiving end for reordering of data.
UDP - User Datagram Protocol: UDP is a simple protocol used for process to process transmission. It is an unreliable, connectionless protocol for applications that do not require flow control or error control. It simply adds port address, checksum and length information to the data it receives from the upper layer.

Question sources

Computer Science model exam · 2015 · Question 43

Question 42 | Q00579

For this hypothetical design, Debre Markos University’s main campus and its Burie agricultural branch are in different towns beyond a single metropolitan area. Which geographic network category connects the two campus LANs?

A. Local Area Network

B. Metropolitan Area Network

C. Personal Area Network

D. Wide Area Network

Hint

Use the cited note definitions to identify the requested function or scope, then check each alternative against that same rule.

Answer D: Wide Area Network

A WAN connects geographically distant networks across regions rather than covering one local site or one metropolitan area. Under the explicit hypothetical placement, the two campus LANs need a WAN connection. A LAN can serve each campus locally, while a MAN covers a metropolitan region and a PAN connects nearby personal devices. The conclusion follows from the stated geography, not the institutions' names or number of computers.

Why each choice is right or wrong

A - Incorrect: A LAN describes local campus connectivity, not the stated inter-town connection.

B - Incorrect: A MAN spans one metropolitan region, excluded by the stated geography.

C - Incorrect: A PAN connects personal nearby devices rather than distant campus networks.

D - Correct: A WAN connects the geographically separated campus LANs.

Primary note proof

Study-note section NET02

> PAN connects personal devices, such as Bluetooth accessories. LAN covers a local building or campus; MAN spans a metropolitan region; WAN connects distant regions. Device count alone does not determine the category. The Internet is a global network of networks, commonly the largest example of a WAN.

Study-note section NET02

> An intranet serves an organization internally; an extranet exposes selected services to approved outsiders. Neither term alone specifies geographic size. A client requests a service; a server supplies it. Peer systems may perform both roles. Dedicated servers concentrate on service workloads but can still be clients of DNS, backup or update services. A ten-user cutoff is a teaching guideline, not a technical law. Centralization simplifies administration but creates dependencies; peer networks still need security.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 22 | lines 26-44

> Personal Area Network (PAN): is a network may be spanned across a given table with distances between the devices not more than few meters. The technology used to interconnect the devices could be a Bluetooth. These networks are called Personal Area Networks, since the devices interconnected in these networks are belongs to a single person.
> Local Area Network (LAN): is a network that may

span across a building, or across several buildings within a single organization, by using intermediate devices, like switches and/or hubs, to interconnect devices in all floors.
Metropolitan Area Network (MAN): is a network that may span across a whole city interconnecting several buildings and organizations.
Wide Area Network (WAN): is a network that may span across multiple cities, or an entire country, or an entire continent or it may even cover the whole world. For example, an Internet is one example of WAN.

Question sources

Computer Science model exam · 2015 · Question 48

Question 43 | Q00582

In OSI reference model, which one is responsible for the translation of incoming and outgoing data .

A. Presentation layer.

B. Application layer.

C. Transport layer.

D. Network layer.

Hint

Match the requested scope or data unit to the layer duties in the note; distinguish hop delivery from end-to-end process delivery.

Answer A: Presentation layer.

Representation translation is explicitly one of presentation-layer duties. Evidence: PDF 16, 16, 16, 15.

Why each choice is right or wrong

A - Correct: Presentation translates data representations (PDF 16, 16, 16, 15.)

B - Incorrect: Application provides network resource access (PDF 16, 16, 16, 15.)

C - Incorrect: Transport delivers between processes (PDF 16, 16, 16, 15.)

D - Incorrect: Network provides logical addressing and routes (PDF 16, 16, 16, 15.)

Primary note proof

Study-note section NET19

OSI session roles establish/manage dialogs and can coordinate checkpoints so transfer resumes after interruption. Presentation roles translate encodings and handle compression/encryption. Compression reduces representation size; encryption hides content and need not shrink it. Application protocols provide services directly to applications. Practical implementations distribute these functions differently; TLS is not proof of a separate physical presentation-layer device.

Study-note section NET17

TCP offers a reliable ordered byte stream using sequence numbers, acknowledgments, retransmission and windows. Flow control protects the receiver; congestion control protects network capacity. UDP sends independent datagrams with ports and a checksum but no built-in setup, delivery guarantee, retransmission or ordering. Live interactive traffic may choose UDP when late data is less useful than lost data. Application protocols can add reliability over UDP.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 16 | lines 33-42

Presentation Layer
• The communicating devices may be having different platforms. The presentation layer performs translation, encryption and compression of data.
• The presentation layer receives the data from the application layer adds header which contains information related to encryption and compression and sends it to the session layer.
• So, the main responsibility of the Presentation layer is translation, compression and encryption.

Data Communication and Computer Networking module | PDF page 16 | lines 43-47

Application Layer
• The application layer enables the user to communicate its data to the receiver by providing certain services.
• The main Responsibility of Application layer is to provide the user access to network resources.

Data Communication and Computer Networking module | PDF page 16 | lines 2-17

• At the sending side, the transport layer receives data from the session layer, divides it into units called segments and sends it to the network layer.
• To ensure process to process delivery the transport layer makes use of port address to identify the data from the sending and receiving process.
• The data can be transported in a connection oriented or connectionless manner.
• The Transport layer is responsible for segmentation and reassembly of the message into segments which

bear sequence numbers.
• The transport layer also carries out flow control and error control functions; but unlike data link layer these are end to end rather than node to node.
• The main responsibility of the transport layer is process to process delivery of the entire message

Data Communication and Computer Networking module | PDF page 15 | lines 41-61

Network Layer
• The network layer makes sure that the data is deliveredto the receiver despite multiple intermediate devices.
• The network layer at the sending side accepts data from the transport layer, divides it into packets, addsaddressing information in the header and passes it tothe data link layer.
• The network layer is responsible for source todestination of delivery of data.
• The network layer uses logical address commonlyknown as IP address to recognize devices on the network.
• Each packet is independent of the other and may travelusing different routes to reach the receiver hence may arrive out of turn at the receiver (Routing).
• The Network layer does not perform any flow controlor error control
• The main responsibility of Network Layer is transmission of packets from source to destination

Question sources

Computer Science model exam · 2015 · Question 51

Question 44 | Q00583

The choice of one topology over the other has an impact on:

A. The capability of the network.

B. The growth of the network.

C. The type of equipment that the network needs.

D. All

Hint

Draw the links and identify shared components, alternate paths and the effect of the specified failure or growth requirement.

Answer D: All

Topology changes cable requirements, central equipment, failure behavior and installation/reconnection costs. The module examples support effects on capability, growth and required equipment. Evidence: PDF 23, 23, 23, 24.

Why each choice is right or wrong

A - Incorrect: Link and failure behavior affect capability (PDF 23, 23, 23, 24.)

B - Incorrect: Cable growth and reconnection costs affect expansion (PDF 23, 23, 23, 24.)

C - Incorrect: A star requires a hub/switch while a mesh requires many direct links (PDF 23, 23, 23, 24.)

D - Correct: All three effects follow from the contrasted layouts (PDF 23, 23, 23, 24.)

Primary note proof

Study-note section NET08

> Bus uses a shared backbone; an unterminated break can disrupt the segment. Star connects endpoints through a central device: one edge failure isolates that endpoint, whereas central failure affects the star. Ring forms a loop; basic single rings are vulnerable to a break, while protected dual rings differ. Token passing is associated with Token Ring but is an access method, not a necessary property of every ring. Tree is hierarchical; hybrid combines arrangements.

Study-note section NET08

> A full undirected mesh of n nodes needs n(n-1)/2 links and n-1 interfaces per node. For 50 nodes: 50×49/2=1225 links. Redundant paths improve fault tolerance at greater cable and interface cost.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 23 | lines 19-34

> Star Topology: in this topology, each node is connected directly to a central device called a hub or a switch. Data on a star network passes through the central device (switch) before continuing to its destination. The central device manages and controls all functions of the network. This configuration is common with twisted pair cable. RJ-45 Connectors are used to connect the cable to the Network Interface Card (NIC) of each computer. Its advantages include, ease of installation and reconfiguration, robust (ease of fault identification and isolation), link failure only affects device(s) connected to that link, and is less expensive than mesh. Its drawbacks include more cable requirements (than bus and ring) and single point of failure (if central device fail, the whole system will be down).

Data Communication and Computer Networking module | PDF page 23 | lines 4-18

Bus Topology: in this topology all devices are connected to a central cable, called the bus or backbone, which is terminated at its ends. The purpose of the terminators is to stop the signal from bouncing, thereby clearing the cable so that other computers can send data. Message transmitted along the Bus is visible to all computers connected to the backbone cable. As the message arrives at each workstation, the workstation checks the destination address contained in the message either to process or drop the packet if it matches or not respectively. Its advantages are, ease of installation and less amount of cable requirement. Its main drawback is, the entire network will be shut down if there is a break in the main cable.

Data Communication and Computer Networking module | PDF page 23 | lines 45-53

Mesh Topology: in this topology devices are connected with many redundant interconnections between network nodes. In a full mesh topology, every node has a connection to every other node in the network, which makes it the most expensive topology over all the other topologies. The number of cables grows fast as the number of nodes increases, and it can be calculated by using the general formula ((n (n - 1)) /2), where n is the number of nodes in the

Data Communication and Computer Networking module | PDF page 24 | lines 2-10

network. It has several benefits, such as: dedicated links between devices, robust (single link failure don‘t affect entire network), privacy/security (direct communication between communicating devices), and ease of fault identification and isolation. Its drawbacks include, installation and reconnection are difficult (large number of cables), huge amount of cables consumes a lot of space, and it is the most expensive of all.

Question sources

Computer Science model exam · 2015 · Question 52

Question 45 | Q00585

One of the following is half-duplex mode of transmission.

A. Walky-talky/policeman phone

B. Television

C. Telephone

D. One-Way Radio

Hint

Compare the signal mechanism, medium properties or transmission direction against the definitions and stated physical assumptions.

Answer A: Walky-talky/policeman phone

Half duplex permits both directions at different times. A conventional walkie-talkie alternates talk and listen, matching this definition. Evidence: PDF 5.

Why each choice is right or wrong

A - Correct: Alternating talk/listen matches half duplex (PDF 5.)

B - Incorrect: Ordinary television broadcast only receives, matching simplex (PDF 5.)

C - Incorrect: An ordinary two-way simultaneous telephone call is full duplex (PDF 5.)

D - Incorrect: One-way radio is simplex (PDF 5.)

Primary note proof

Study-note section NET06

> Simplex is one way, half duplex alternates directions, and full duplex permits simultaneous sending/receiving. A walkie-talkie is half duplex; a telephone conversation uses full duplex. Serial sends sequential bits; parallel uses multiple conductors and may suffer skew. Character-oriented asynchronous serial adds start/stop bits; synchronous framing uses ongoing clock recovery. Neither is synonymous with browser asynchronous requests.

Study-note section NET06

> Transmission delay is packet bits divided by link bit rate; propagation delay is distance divided by signal speed. Processing and queueing add delay. A 1000-byte packet takes 0.8 ms to serialize at 10 Mbit/s; increasing line rate does not reduce propagation time.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 5 | lines 43-48

> • Simplex: Only one of the devices sends the data and the
> other one only receives the data (Unidirectional).
> • Half Duplex: both the stations can transmit as well as
> receive but not at the same time.

• Full duplex mode: both stations can transmit and receive at the same time.

Question sources

Computer Science model exam · 2015 · Question 54

Question 46 | Q00588

VPN is abbreviated as

A. Visual Private Network

B. Virtual Private Network

C. Virtual Protocol Network

D. Virtual Protocol Networking

Hint

Find the full expansion in the terminology note and compare each word rather than only matching initials.

Answer B: Virtual Private Network

NET11 expands VPN as Virtual Private Network and describes the logical private connection it provides over another network. The word Virtual matters because the connection is logically overlaid rather than necessarily a separate physical private network. The alternatives replace parts of the established expansion with visual or protocol and therefore do not match the note.

Why each choice is right or wrong

A - Incorrect: Visual substitutes an unrelated word for Virtual in the established VPN expansion.

B - Correct: Virtual Private Network is the exact expansion given in NET11.

C - Incorrect: Protocol replaces Private, changing the acronym expansion away from the defined term.

D - Incorrect: Protocol Networking is not the defined Private Network phrase in VPN.

Primary note proof

Study-note section NET11

A firewall allows, rejects or inspects traffic under a security policy; it does not necessarily encrypt. A VPN, Virtual Private Network, provides a logical private connection over another network; a secure VPN authenticates/encrypts its tunnel. A modem modulates outgoing and demodulates incoming carrier signals. These functions may coexist in one home router but remain conceptually distinct.

Study-note section NET11

Routers forward IP packets between networks using destination prefixes and next hops. They separate broadcast domains and normally do not forward local link broadcasts. A default gateway is usually a router, while a protocol gateway can translate application formats; therefore a gateway is not inherently a device that implements every OSI layer.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 22 | lines 2-19

A network can be defined as two or more computers connected together in such a way that they can share resources. The primary purpose of a network is to share resources, and a resource could be:
• a file,
• a folder,
• a printer,
• a disk drive, or just about anything else that exists on a computer.
Therefore, a computer network is simply a collection of computers or other hardware devices that are connected together, either physically or logically, using special hardware and software, to allow them to exchange information and cooperate. Networking is the term that describes the processes involved in designing, implementing, upgrading, managing and otherwise working with networks and network technologies.

Question sources

Computer Science model exam · 2015 · Question 57

Question 47 | Q00596

How many equal /27 subnets can be created from 192.168.20.0/24, counting every subnet?

A. 8

B. 16

C. 32

D. 64

Hint

Convert the mask to a prefix, separate network and host bits, and apply the relevant subnet-count or usable-host rule.

Answer A: 8

Subnet counts depend on both the parent and child prefixes. Dividing a /24 parent into /27 children borrows three bits, giving 2^3 = 8 subnets. Each child has five host bits and therefore 32 total addresses, but that address count is a different quantity. Counting every subnet avoids the obsolete practice of excluding the first and last subnet.

Why each choice is right or wrong

A - Correct: Three borrowed bits produce eight /27 subnets.

B - Incorrect: Sixteen would require four borrowed bits, not three.

C - Incorrect: Thirty-two is the number of addresses in each /27, not the number of children of this /24.

D - Incorrect: Sixty-four requires six borrowed bits rather than three.

Primary note proof

Study-note section NET26

> To split parent /a into equal /p blocks, borrow b=p-a bits and obtain 2^b subnets. Do not subtract two subnets under modern practice. For a Class B /16 parent split to /19, b=3 gives eight subnets, each with 8192 addresses and 8190 conventional hosts. A /19 alone does not state its parent.

Study-note section NET26

> For H hosts, choose the smallest h satisfying 2^h-2≥H, then p=32-h. For 24 hosts use /27; 52 or 57 use /26; 100 use /25; 500 use /23. For at least six equal subnets choose b=3. A Class C /24 split to /27 yields eight subnets. Always check both the number of subnets and the host capacity.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 18 | lines 45-54

> IP addresses: IP address uniquely identifies a device on the
> Internet. Every host and router on the Internet has an IP address,
> which encodes its network number and host number.
> • The combination is unique: in principle, no two
> machines on the Internet have the same IP address.
> • An IPv4 address is 32 bits long
> • They are used in the Source address and Destination
> address fields of IP packets.
> • An IP address does not refer to a host but it refers to a
> network interface.

Data Communication and Computer Networking module | PDF page 19 | lines 23-36

> Classful addressing : In classful addressing, the
> addressspace is divided into five classes: A, B, C,
> D, and E.
> • Netid and Hostid In classful addressing, an IP

addressin class A, B, or C is divided into netid
and hostid.
Subnetting: It allows a network to be split into several
parts for internal use but still act like a single network to
the outsideworld.
• To implement subnetting, the router needs a
subnet mask that indicates the split between
network + subnet number and host. Ex.
255.255.252.0/22. A‖/22‖ to indicate that the
subnet mask is 22 bits long.

Data Communication and Computer Networking module | PDF page 19 | lines 37-44

CIDR: A class B address is far too large for most
organizationsand a class C network, with 256 addresses is
too small. This leads to granting Class B address to
organizations who do not require all. This is resulting in
depletion of Address space. A solution is CIDR (Classless
InterDomain Routing) The basic idea behind CIDR, is to
allocate the remaining IP addresses in variable-sized
blocks, without regard to the classes.

Question sources

Computer Science model exam · 2015 · Question 65

Question 48 | Q00601

Given an IP Address 172.16.28.252 with the subnet mask of 255.255.240.0 what is the correct network address?

A. 172.16.24.0

B. 172.16.28.0

C. 172.16.0.0

D. 172.16.16.0

Hint

Convert the mask to a prefix, separate network and host bits, and apply the relevant subnet-count or usable-host rule.

Answer D: 172.16.16.0

240=11110000 in the third mask octet. 28 (00011100) AND 240 (11110000)=16 (00010000); the last masked octet is zero. Thus the network is 172.16.16.0. Evidence: PDF 18, 19, 19.

Why each choice is right or wrong

A - Incorrect: 24 is not aligned to a 16-wide third-octet block (PDF 18, 19, 19.)

B - Incorrect: 28 retains host bits instead of masking them (PDF 18, 19, 19.)

C - Incorrect: 0 would discard the retained third-octet network bit (PDF 18, 19, 19.)

D - Correct: 16 is the result of the mask operation (PDF 18, 19, 19.)

Primary note proof

Study-note section NET24

A /p IPv4 prefix has p leading one bits followed by 32-p zeros. Partial octet masks are 128,192,224,240,248,252,254. /19 is 255.255.224.0; /20 is 255.255.240.0; /21 is 255.255.248.0, correcting the study guide's 255.248.0.0 mistake.

Study-note section NET24

Compute network=address AND mask. Host bits zero identify the block start; host bits one give broadcast. With 172.16.28.252/20, the third octet is grouped in blocks of 16, so the network is 172.16.16.0 and broadcast 172.16.31.255. A written host/prefix such as 172.105.180.0/21 need not be an aligned block label: masking yields 172.105.176.0/21.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 18 | lines 45-54

IP addresses: IP address uniquely identifies a device on the
Internet. Every host and router on the Internet has an IP address,
which encodes its network number and host number.
• The combination is unique: in principle, no two
machines on the Internet have the same IP address.
• An IPv4 address is 32 bits long
• They are used in the Source address and Destination
address fields of IP packets.
• An IP address does not refer to a host but it refers to a
network interface.

Data Communication and Computer Networking module | PDF page 19 | lines 2-22

Address Space: An address space is the total
number ofaddresses used by the protocol.
• If a protocol uses N bits to define an address,
the address space is 2N
because each bit can
have twodifferent values (0 or 1) and N bits
can have 2N values.
• IPv4 uses 32-bit addresses, which means that
the address space is 232 or 4,294,967,296
(more than 4billion).
Notations: There are two notations to show an IPv4 address:
• Binary notation: The IPv4 address is displayed
as 32bits. ex. 11000001 10000011 00011011

11111111
• Dotted decimal notation: To make the IPv4 address easier to read, Internet addresses are usually written in decimal form with a decimal point (dot) separatingthe bytes. Each byte (octet) is 8 bits hence each number in dotted-decimal notation is a value rangingfrom 0 to 255. Ex. 129.11.11.239

Data Communication and Computer Networking module | PDF page 19 | lines 23-36

Classful addressing : In classful addressing, the addressspace is divided into five classes: A, B, C, D, and E.
• Netid and Hostid In classful addressing, an IP addressin class A, B, or C is divided into netid and hostid.
Subnetting: It allows a network to be split into several parts for internal use but still act like a single network to the outsideworld.
• To implement subnetting, the router needs a subnet mask that indicates the split between network + subnet number and host. Ex. 255.255.252.0/22. A‖/22‖ to indicate that the subnet mask is 22 bits long.

Question sources

Computer Science model exam · 2015 · Question 70

Question 49 | Q00602

One of the following is true about packet switching.

A. Packets travel around the network seeking out the most efficient route.

B. Packets should necessarily seek out the shortest route.

C. The message gets broken into small data packets.

D. All

Hint

Compare signal repetition, frame forwarding, packet routing and policy enforcement using the stated device or traffic assumptions.

Answer C: Packet switching divides a message into packets

The defining packet-switching property is dividing data into packets for shared-link forwarding. Routing may seek good paths, but packets do not guarantee the most efficient or geometrically shortest path. C directly states the definition; D includes unsupported universal route claims and therefore fails.

Why each choice is right or wrong

A - Incorrect: Routing chooses next hops, but packet switching does not guarantee packets discover the globally most efficient route.

B - Incorrect: Packets are not guaranteed to take the geometrically shortest route.

C - Correct: Breaking a message into data packets is the packet-switching operation.

D - Incorrect: The all option includes unsupported route-optimality and necessary-shortest-path claims.

Primary note proof

Study-note section NET31

> Circuit switching sets up a path with reserved resources, transfers data, then releases it. Predictable allocated bandwidth trades against setup/blocking and wasted reservation during silence. A traditional telephone call is the standard example. Packet switching divides data into packets that share links statistically; queueing can add variable delay and loss. This does not make modern voice-over-packet impossible: buffering, scheduling and capacity planning manage it.

Study-note section NET31

> Datagram packets are forwarded independently. Virtual circuits establish forwarding state, but resource reservation is optional, not a necessary property of every virtual circuit. Message switching stores a complete message before forwarding, without a dedicated end-to-end path. Packet store-and-forward waits for the full packet/frame; cut-through starts after enough header arrives; fragment-free historically waits through the initial collision-sensitive portion. No routing algorithm guarantees that every packet always takes the geometrically shortest route.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 15 | lines 41-61

> Network Layer
> • The network layer makes sure that the data is deliveredto the receiver despite multiple intermediate devices.
> • The network layer at the sending side accepts data from the transport layer, divides it into packets, addsaddressing information in the header and passes it tothe data link layer.
> • The network layer is responsible for

source todestination of delivery of data.
• The network layer uses logical address commonlyknown as IP address to recognize devices on the network.
• Each packet is independent of the other and may travelusing different routes to reach the receiver hence may arrive out of turn at the receiver (Routing).
• The Network layer does not perform any flow controlor error control
• The main responsibility of Network Layer is transmission of packets from source to destination

Data Communication and Computer Networking module | PDF page 20 | lines 27-36

Message Switching:
Packet Switching: Packet switching was designed to address the shortcomings of circuit switching in dealing with data communication. Unlike circuit switching where communication is continuous along a dedicated circuit, in packet switching, communication is discrete in form of packets.
The three switching modes to choose from are:
• Cut-through
• Store-and-forward
• Fragment-free

Question sources

Computer Science model exam · 2015 · Question 71

Question 50 | Q00603

Which statements correctly compare the seven-layer OSI reference model with the four-layer TCP/IP model? Select all that apply.

A. Both have application layers.

B. Both have comparable transport and network layers.

C. Both uses packet-switching instead of circuit-switching technology.

D. All

Hint

Match the requested scope or data unit to the layer duties in the note; distinguish hop delivery from end-to-end process delivery.

Answer A, B: Both have application layers.; Both have comparable transport and network layers.

Both models include application responsibilities and corresponding transport and network functions. TCP/IP groups the OSI session, presentation and application responsibilities into its application layer, and calls its network layer the Internet layer. An abstract reference model does not itself execute a switching technology. Consequently, the claim that both models necessarily use packet switching is not a valid shared model property.

Why each choice is right or wrong

A - Correct: Both models include an application layer, although TCP/IP folds several OSI upper-layer functions into it.

B - Correct: TCP/IP retains transport and maps OSI network responsibilities to its Internet layer.

C - Incorrect: A reference model does not itself use a switching technology or restrict every implementation to one.

D - Incorrect: The implemented-technology claim in C is not a property established for both abstract models.

Primary note proof

Study-note section NET19

> The four-layer TCP/IP model folds OSI layers 5-7 into application, retains transport, calls layer 3 Internet, and combines link/physical as network access. A model is a guide to functions, not a guarantee that every application gets a reliable network. Distinguish end-to-end application service from its underlying process-to-process transport.

Study-note section NET03

> A reference model divides responsibilities and interfaces; it is not itself executable networking software. OSI is a seven-layer reference model; TCP/IP describes an implemented protocol suite, usually taught with four layers. A five-layer teaching model separates physical and link functions. State the model before counting layers.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 17 | lines 3-15

> The structure TCP/IP model is very similar to the
> structure of the OSI reference model. The OSI model has
> seven layers where the TCP/IP model has four layers.
> • The Application layer of TCP/IP model
> corresponds to the Application Layer of Session,
> Presentation & Application Layer of OSI model.
> • The Transport layer of TCP/IP model corresponds
> to theTransport Layer of OSI model
> • The Network layer of TCP/IP model corresponds
> to the Network Layer of OSI model

• The Host to network layer of TCP/IP model correspondsto the Physical and Data link Layer of OSI model.

Data Communication and Computer Networking module | PDF page 16 | lines 50-59

After understanding the concept of layered task and the OSI model, we introduce the TCP/IP model. This model is currently being used on our systems. TCP/IP model is a collection of protocols often called a protocol suite. It offers a rich variety of protocols.
It is a hierarchical model; it existed even before the OSI model was developed. Originally had four layers (bottom to top):
1. Host to Network Layer
2. Internet Layer
3. Transport Layer

Question sources

Computer Science model exam · 2015 · Question 72

Question 51 | Q00604

One of the following is network layer protocol.

A. HTTP

B. FTP

C. ARP

D. TCP

Hint

Match the requested scope or data unit to the layer duties in the note; distinguish hop delivery from end-to-end process delivery.

Answer C: ARP

Within this module, ARP is grouped among protocols supporting IP at the network layer. This follows the assigned taxonomy rather than assuming that all taxonomies place ARP identically. Evidence: PDF 17, 17, 18, 18.

Why each choice is right or wrong

A - Incorrect: HTTP is an application service in the table (PDF 17, 17, 18, 18.)

B - Incorrect: FTP is application file transfer (PDF 17, 17, 18, 18.)

C - Correct: ARP is explicitly grouped under network/IP support (PDF 17, 17, 18, 18.)

D - Incorrect: TCP belongs to transport (PDF 17, 17, 18, 18.)

Primary note proof

Study-note section NET20

ARP resolves an on-link IPv4 next hop to a link address, using a broadcast request and normally unicast reply. For an off-subnet target, ARP resolves the gateway, not the remote target's MAC. It bridges the network/link addressing boundary and is often classified at the link layer; calling ARP simply a network protocol uses a loose textbook convention. RARP reverses hardware-to-IP lookup; BOOTP/DHCP support boot configuration. ICMP reports errors and diagnostics; IGMP manages IPv4 multicast membership. These are separate companion protocols, not four pieces whose combination is IP.

Study-note section NET21

HTTP defines web request/response semantics; it is stateless, and a message body may be absent. HTTPS adds TLS protection. FTP transfers files using control and separate data connections; it is not the same protocol as SFTP. SMTP submits and relays mail; POP3 retrieves messages and IMAP accesses/synchronizes server mailboxes. Saying SMTP handles both sending and end-user mailbox retrieval is inaccurate.

Study-note section NET17

TCP offers a reliable ordered byte stream using sequence numbers, acknowledgments, retransmission and windows. Flow control protects the receiver; congestion control protects network capacity. UDP sends independent datagrams with ports and a checksum but no built-in setup, delivery guarantee, retransmission or ordering. Live interactive traffic may choose UDP when late data is less useful than lost data. Application protocols can add reliability over UDP.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 17 | lines 22-38

Network Layer or IP
Also called as the Internetwork Layer (IP). It holds the IP protocol which is a network layer protocol and is responsiblefor source to destination transmission of data.
The Internetworking Protocol (IP) is a connection-less & unreliable protocol.
It is a best effort delivery service. i.e. there is no error checking in IP, it simply sends the data and relies on its underlying layers to get the data transmitted to the destination.Even if it is unreliable IP cannot be considered weak and useless; since it provides only the functionality that is requiredfor transmitting data thereby giving maximum efficiency.
Since there is no mechanism of error detection or correction in IP, there will be no delay introduced on a medium where thereis no error at all.

Data Communication and Computer Networking module | PDF page 17 | lines 44-53

ARP - Address Resolution Protocol: It is used to resolve thephysical address of a device on a network, where its logical address is known.
Physical address is the 48 bit address that is imprinted on theNIC or LAN card, Logical address is the Internet Address orcommonly known as IP address that is used to uniquely & universally identify a device.
RARP- Reverse Address Resolution Protocol: It is used bya device on the network to find its Internet address when it knows its physical address.

Data Communication and Computer Networking module | PDF page 18 | lines 27-32

Application Layer
The Application Layer is a combination of Session, Presentation & Application Layers of OSI models and defines high level protocols like File Transfer (FTP), Electronic Mail (SMTP), Virtual Terminal (TELNET), Domain Name Service (DNS), etc.

Data Communication and Computer Networking module | PDF page 18 | lines 9-21

TCP - Transmission Control Protocol: TCP is a reliable connection-oriented, reliable protocol. i.e. a connection is established between the sender and receiver before the data can be transmitted. It divides the data it receives from the upper layer into segments and tags a sequence number to each segment which is used at the receiving end for reordering of data.
UDP - User Datagram Protocol: UDP is a simple protocol used for process to process transmission. It is an unreliable, connectionless protocol for applications that do not require flow control or error control. It simply adds port address, checksum and length information to the data it receives from the upper layer.

Question sources

Computer Science model exam · 2015 · Question 73

Question 52 | Q00629

One of the following is responsible for receiving and transmitting the signals across the physical media.

A. Datalink Layer

B. Physical layer

C. Application Layer.

D. Transport Layer.

Hint

Compare the signal mechanism, medium properties or transmission direction against the definitions and stated physical assumptions.

Answer B: Physical layer

Transmission of signals across a physical medium is explicitly the physical-layer task. Evidence: PDF 14, 15, 16, 16.

Why each choice is right or wrong

A - Incorrect: Data link frames data and controls access (PDF 14, 15, 16, 16.)

B - Correct: Physical converts bits to signals and sends them (PDF 14, 15, 16, 16.)

C - Incorrect: Application supplies user network services (PDF 14, 15, 16, 16.)

D - Incorrect: Transport manages process delivery (PDF 14, 15, 16, 16.)

Primary note proof

Study-note section NET09

> A NIC supplies a computer’s network interface and commonly implements both physical and link functions. Calling a NIC a physical interface does not mean all its functions are layer 1. Physical specifications include connectors, signaling, voltage, timing and physical coding/modulation; the PHY interface to MAC handles hardware signaling.

Study-note section NET12

> Sending proceeds from application data to transport segment/datagram, network packet, link frame and physical bits/symbols; receiving reverses the order. Each layer serves the layer above. A router removes a received link frame, inspects IP, and creates a new link frame for the next hop. MAC addresses usually change across routed hops; end-to-end IP addresses ordinarily remain until translation.

Study-note section NET17

> TCP offers a reliable ordered byte stream using sequence numbers, acknowledgments, retransmission and windows. Flow control protects the receiver; congestion control protects network capacity. UDP sends independent datagrams with ports and a checksum but no built-in setup, delivery guarantee, retransmission or ordering. Live interactive traffic may choose UDP when late data is less useful than lost data. Application protocols can add reliability over UDP.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 14 | lines 32-49

> Physical Layer:
> • The Physical Layer provides a standardized interface to physical transmission media, including: Mechanical specification of electrical connectors and cables, for example maximum cable length, Electrical specification

of transmission line and Bit-by-bit or symbol-by-symbol delivery.
• Interface: The Physical Layer defines the characteristics of interfaces between the devices & transmission medium.
• Representation of bits: The physical layer is concerned with transmission of signals from one device to another which involves converting data (1_s & 0_s) into signals and vice versa. It is not concerned with the meaning or interpretation of bits.
• Data rate: The physical layer defines the data transmission rate i.e. number of bits sent per second. It is the responsibility of the physical layer to maintain the defined data rate.

Data Communication and Computer Networking module | PDF page 15 | lines 13-40

Data Link Layer
• The Data Link layer adds reliability to the physical layer by providing error detection and correction mechanisms.
• Framing: the Data Link layer receives the data from Network Layer and divides the stream of bits into fixed size manageable units called as Frames and sends it to the physical layer. On the receiver side, the data link layer receives the stream of bits from the physical layer and regroups them into frames and sends them to the Network layer.
• Physical Addressing: The Data link layer appends the physical address in the header of the frame before sending it to physical layer.
• Flow control: The data link layer makes sure that the sender sends the data at a speed at which the receiver canreceive it else if there is an overflow at the receiver sidethe data will be lost.
• Error Control: The data link layer imposes error control mechanism to identify lost or damaged frames, duplicateframes and then retransmit them.
• Access Control: The data link layer imposes access control mechanism to determine which device has right to send data in an multipoint connection setting.
• Main Responsibility: The main responsibility of the data link layer is hop to hop transmission of frames.

Data Communication and Computer Networking module | PDF page 16 | lines 43-47

Application Layer
• The application layer enables the user to communicate its data to the receiver by providing certain services.
• The main Responsibility of Application layer is to provide the user access to network resources.

Data Communication and Computer Networking module | PDF page 16 | lines 2-17

• At the sending side, the transport layer receives data from the session layer, divides it into units called segments and sends it to the network layer.
• To ensure process to process delivery the transport layer makes use of port address to identify the data from the sending and receiving process.
• The data can be transported in a connection oriented or connectionless manner.
• The Transport layer is responsible for segmentation and reassembly of the message into segments which bear sequence numbers.
• The transport layer also carries out flow control and error control functions; but unlike data link layer these are end to end rather than node to node.
• The main responsibility of the transport layer is process to process delivery of the entire message

Question sources

Computer Science model exam · 2015 · Question 98

Question 53 | Q00636

Which listed device performs layer-1 signal regeneration without inspecting destination addresses?

A. Router

B. Switch

C. Firewall

D. Repeater

Hint

Match the requested scope or data unit to the layer duties in the note; distinguish hop delivery from end-to-end process delivery.

Answer D: Repeater

A repeater regenerates physical signals and therefore performs a layer-1 function. Routers decide where to forward network-layer packets, and ordinary Ethernet switches make link-layer decisions using MAC addresses. A firewall enforces a security policy rather than defining a physical signal-regeneration role. Replacing the duplicated firewall distractor restores a meaningful physical-layer choice without changing the layer-identification concept.

Why each choice is right or wrong

A - Incorrect: A router's defining forwarding function is network-layer IP routing rather than layer-1 signal repetition.

B - Incorrect: An ordinary Ethernet switch performs layer-2 MAC frame forwarding.

C - Incorrect: A firewall enforces traffic policy rather than being the layer-1 repeater/hub requested.

D - Correct: A repeater regenerates layer-1 signals without inspecting destination addresses.

Primary note proof

Study-note section NET09

> A repeater regenerates layer-1 signals without inspecting destination addresses. An active hub is a multiport repeater: it repeats incoming signals onto other ports, placing half-duplex endpoints in one collision domain. A passive hub is a connector. A hub neither learns MAC addresses nor eliminates collisions. An endpoint such as a network printer consumes services; routers, hubs and access points are intermediary devices.

Study-note section NET10

> A bridge or ordinary Ethernet switch operates at layer 2. It learns source-MAC-to-port mappings, looks up the destination, forwards a known unicast to its port, filters it if the destination is on the incoming segment, and floods an unknown unicast or broadcast within its VLAN. A switch does not always send only to one destination port. Wireless access points normally bridge wireless and wired link-layer traffic.

Study-note section NET11

> A firewall allows, rejects or inspects traffic under a security policy; it does not necessarily encrypt. A VPN, Virtual Private Network, provides a logical private connection over another network; a secure VPN authenticates/encrypts its tunnel. A modem modulates outgoing and demodulates incoming carrier signals. These functions may coexist in one home router but remain conceptually distinct.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 12 | lines 17-26

> Active Hubs
> An active hub is actually a multipart repeater. It is
> normallyused to create connections between stations in

a physical startopology.
HUB: Hubs are commonly used to connect segments (devices)of a LAN. Hubs don‘t filter information; instead broadcast incoming packets to all computers connected to it. A hub contains multiple ports which support 8, 12 or 24 RJ-45 ports. Two types: Passive hub and Active hub. It is used in star or ring topology.

Data Communication and Computer Networking module | PDF page 12 | lines 27-37

SWITCH: A switch filters and forwards data packets across anetwork.
Unlike a hub which simply replicates what it receives on oneport onto all the other ports, a switch keeps a record of the MAC addresses of the devices attached to it.
When the switch receives a data packet, it forwards the packetdirectly to the recipient device by looking up the MAC address.
• Switch is intelligent and expensive than Hub
• Switch is a point to point communication device
• Hub is a broadcasting device

Data Communication and Computer Networking module | PDF page 12 | lines 38-52

ROUTER: Router is a specialized network device used tointerconnect different types of network that uses different protocol.
Router allows the users to connect several LAN and WAN
• A LAN to another LAN
• A WAN to another WAN
• A LAN to the Internet
Routers use the routing table to determine how to forwardpackets.
• The list of routing tables provides directions to transfer the data to a particular network destination -various paths to forward the data.
• A router analyzes a destination IP address of a givenpacket and compares it with the routing table to decide the packet's next best path

Data Communication and Computer Networking module | PDF page 11 | lines 54-55

Repeater: A repeater is a device that operates only in the physical layer. A repeater receives a signal and, before it

Question sources

Computer Science model exam · 2015 · Question 105

Question 54 | Q00637

A data communication component that helps to convert data into transmittable signal.

A. Transmission media

B. Transmitter

C. Receiver

D. Data source

Hint

Compare the signal mechanism, medium properties or transmission direction against the definitions and stated physical assumptions.

Answer B: Transmitter

NET01 separates creating data, converting it to a signal, carrying that signal and reconstructing the data. The stem asks specifically about the conversion into a transmittable signal, which is the transmitter's role. A source supplies the data before this conversion, while the receiver performs the reconstruction at the far end.

Why each choice is right or wrong

A - Incorrect: The transmission medium carries the signal; it is not the component that converts source data into it.

B - Correct: The transmitter converts data into a signal suitable for transmission over the medium.

C - Incorrect: The receiver reconstructs data from the incoming signal, performing the opposite end's role.

D - Incorrect: The data source creates the data; signal conversion is assigned separately to the transmitter.

Primary note proof

Study-note section NET01

> Data are raw representations; information is data interpreted for a purpose. Communication requires a message, sender, receiver, medium and agreed protocol. A source creates data; a transmitter converts it to a signal; a receiver reconstructs data. Distance affects engineering but is not a sixth component.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 10 | lines 36-55

> TRANSMISSION MEDIA
> Transmission media is a means by which a
> communicationsignal is carried from one system to
> another

A transmission medium can be defined as anything that cancarry information from a source to a destination. The transmission medium is usually free space, metallic cable orfiber optic cable. Guided and Unguided (WIRELESS) Guided Transmission Media uses a cabling system that guidesthe data signals along a specific path. Out of these twisted-paircable, coaxial cable transport signals in the form of electricsignals and fiber-optic cable transport signals in the form oflight. Unguided Transmission Media transport data without using a physical conductor. It uses wireless electromagnetic signals to send data. Three types of unguided media:
• Radio waves
• Micro waves
• Infrared.

Data Communication and Computer Networking module | PDF page 14 | lines 32-49

Physical Layer:
• The Physical Layer provides a standardized interface to physical transmission media, including: Mechanical specification of electrical connectors and cables, for example maximum cable length, Electrical specification of transmission line and Bit-by-bit or symbol-by-symbol delivery.
• Interface: The Physical Layer defines the characteristics of interfaces between the devices & transmission medium.
• Representation of bits: The physical layer is concerned with transmission of signals from one device to another which involves converting data (1_s & 0_s) into signals and vice versa. It is not concerned with the meaning or interpretation of bits.
• Data rate: The physical layer defines the data transmission rate i.e. number of bits sent per second. It is the responsibility of the physical layer to maintain the defined data rate.

Data Communication and Computer Networking module | PDF page 5 | lines 23-35

A Data Communication system has five components:-
• Message:- is the information to be communicated by the sender to the receiver.
• Sender The sender is any device that is capable of sending the data (message).
• Receiver: - is a device that the sender wants to communicate the data (message).
• Transmission Medium: - It is the path by which the

message travels from sender to receiver. It can be wired or wireless and many subtypes in both.
• Protocol:- It is an agreed upon set or rules used by the sender and receiver to communicate data. Rules that govern data communication.

Question sources

Computer Science model exam · 2015 · Question 106

Question 55 | Q00638

Among the following one is the responsibility of logical link control layer.

A. Identify the network layer protocol.

B. Marking the beginning and ending of the frame.

C. Addressing the frame.

D. All

Hint

Match the requested scope or data unit to the layer duties in the note; distinguish hop delivery from end-to-end process delivery.

Answer A: Identify or multiplex the network-layer protocol

LLC identifies or multiplexes the upper-layer protocol carried over the link. NET13 assigns medium-dependent addressing/access and frame delivery to MAC, and says exact framing depends on the protocol. Therefore the specific LLC duty offered here is identifying the network-layer protocol; the other functions cannot all be attributed to LLC.

Why each choice is right or wrong

A - Correct: Identifying or multiplexing an upper-layer network protocol is an explicit LLC responsibility in NET13.

B - Incorrect: Beginning/end frame delimitation belongs to protocol-specific framing, not the distinguishing LLC upper-protocol identification function.

C - Incorrect: Medium-dependent frame addressing belongs to MAC rather than the LLC duty asked about.

D - Incorrect: The all option incorrectly includes frame addressing and delimitation as specifically LLC responsibilities.

Primary note proof

Study-note section NET13

Link-layer LLC identifies or multiplexes upper-layer protocols and may supply link control; MAC handles medium-dependent addressing/access and frame delivery. Network addressing belongs

to layer 3. Ethernet, PPP and HDLC are link protocols. Frame headers may carry addresses and control/type fields; synchronization and exact framing depend on the protocol.

Study-note section NET12

Sending proceeds from application data to transport segment/datagram, network packet, link frame and physical bits/symbols; receiving reverses the order. Each layer serves the layer above. A router removes a received link frame, inspects IP, and creates a new link frame for the next hop. MAC addresses usually change across routed hops; end-to-end IP addresses ordinarily remain until translation.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 15 | lines 13-40

Data Link Layer
• The Data Link layer adds reliability to the physical layer by providing error detection and correction mechanisms.
• Framing: the Data Link layer receives the data from Network Layer and divides the stream of bits into fixed size manageable units called as Frames and sends it to the physical layer. On the receiver side, the data link layer receives the stream of bits from the physical layer and regroups them into frames and sends them to the Network layer.
• Physical Addressing: The Data link layer appends the physical address in the header of the frame before sending it to physical layer.
• Flow control: The data link layer makes sure that the sender sends the data at a speed at which the receiver canreceive it else if there is an overflow at the receiver sidethe data will be lost.
• Error Control: The data link layer imposes error control mechanism to identify lost or damaged frames, duplicateframes and then retransmit them.
• Access Control: The data link layer imposes access control mechanism to determine which device has right to send data in an multipoint connection setting.
• Main Responsibility: The main responsibility of the data link layer is hop to hop transmission of frames.

Data Communication and Computer Networking module | PDF page 21 | lines 6-26

MEDIUM ACCESS CONTROL
The problem of controlling the access to the medium is similarto the rules of speaking in a meeting (the right

to speak isupheld; two people do not speak at the same time; do notinterrupt each other; do not monopolize the discussion; ...) Three categories of multiple access protocols
Random Access Protocols - try your best like taxis do
• MA - Multiple Access
• CSMA - Carrier Sense MA
• CSMA/CD - CSMA with Collision Detection
• CSMA/CA - CSMA with Collision AvoidanceControlled-Access Protocols - get permission
• Reservation
• Polling
• Token Passing
Channelization Protocols - simultaneous use
• FDMA - Frequency-Division MA
• TDMA - Time-Division MA
• CDMA - Code-Division MA

Question sources

Computer Science model exam · 2015 · Question 107

Question 56 | Q00639

One of the following is ODD

A. 192.257.10.0

B. 192.168.10.0

C. 172.16.1.1

D. 192.168.0.0

Hint

Use the cited note definitions to identify the requested function or scope, then check each alternative against that same rule.

Answer A: 192.257.10.0

As a syntactic IPv4 address comparison, 257 exceeds the permitted 0-255 octet range. The others have four legal octets; no host mask is supplied to test host assignability. Evidence: PDF 19.

Why each choice is right or wrong

A - Correct: 257 violates the octet limit (PDF 19.)

B - Incorrect: All octets fall between 0 and 255 (PDF 19.)

C - Incorrect: All octets fall between 0 and 255 (PDF 19.)

D - Incorrect: All octets fall between 0 and 255 (PDF 19.)

Primary note proof

Study-note section NET22

> Write IPv4 as four decimal octets 0-255, or as 32 binary bits. Use weights 128,64,32,16,8,4,2,1 within each octet. Thus 11000001 10000011 00011011 11111111 is 193.131.27.255. A value such as 257 is impossible. Syntactic validity differs from assignability: an address ending .0 or .255 can be a host under some prefixes.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 19 | lines 2-22

> Address Space: An address space is the total
> number ofaddresses used by the protocol.
> • If a protocol uses N bits to define an address,
> the address space is 2N
> because each bit can
> have twodifferent values (0 or 1) and N bits
> can have 2N values.
> • IPv4 uses 32-bit addresses, which means that
> the address space is 232 or 4,294,967,296
> (more than 4billion).
> Notations: There are two notations to show an IPv4 address:
> • Binary notation: The IPv4 address is displayed
> as 32bits. ex. 11000001 10000011 00011011
> 11111111
> • Dotted decimal notation: To make the IPv4
> address easier to read, Internet addresses are
> usually written in decimal form with a decimal
> point (dot) separatingthe bytes. Each byte (octet)
> is 8 bits hence each number in dotted-decimal
> notation is a value rangingfrom 0 to 255. Ex.
> 129.11.11.239

Question sources

Computer Science model exam · 2015 · Question 108

Question 57 | Q00640

The most commonly used method to convert analog data to digital form.

A. Line coding scheme

B. Data encoding

C. Pulse code modulation

D. Demodulation

Hint

Use the cited note definitions to identify the requested function or scope, then check each alternative against that same rule.

Answer C: Pulse code modulation (PCM)

NET15 identifies PCM as the analog-to-digital procedure of sampling the analog input, quantizing each sample and encoding its level as bits. The note does not establish comparative usage statistics, but PCM is the specific conversion method among the choices. Line coding maps existing digital bits to signals; demodulation recovers information from a carrier rather than necessarily digitizing analog data.

Why each choice is right or wrong

A - Incorrect: Line coding begins with digital bits and maps them to digital signal patterns, rather than digitizing analog input.

B - Incorrect: Data encoding is a broad description and does not identify the specific analog-digitization method supplied here.

C - Correct: PCM performs the sampling, quantization and binary encoding needed to turn analog input into digital data.

D - Incorrect: Demodulation removes carrier modulation; it does not itself specify analog-to-digital sampling and quantization.

Primary note proof

Study-note section NET15

> ASK varies carrier amplitude, FSK frequency, PSK phase; QAM combines amplitude and phase. AM/FM/PM can carry analog data. PCM digitizes analog input by sampling, quantizing and encoding. Sampling must exceed twice the highest retained baseband frequency in practical designs; b-bit samples have 2^b quantization levels and uncompressed rate fs×b. PAM/PWM are pulse modulation methods; pulse amplitude or width alone is not a binary PCM code.

Study-note section NET15

> Line coding maps digital bits to digital signal patterns. NRZ uses levels without a forced mid-bit return; Manchester supplies a mid-bit transition for clocking, with bit convention specified. Differential Manchester encodes using transitions relative to previous state. AMI alternates the polarity of successive ones; pseudoternary alternates zero pulses. Block coding adds code redundancy; scrambling replaces problematic patterns without necessarily increasing bit count. Multilevel schemes include 2B1Q and 8B6T; MLT-3 uses a sequence of voltage transitions.

Study-note section NET11

> A firewall allows, rejects or inspects traffic under a security policy; it does not necessarily encrypt. A VPN, Virtual Private Network, provides a logical private connection over another network; a secure VPN authenticates/encrypts its tunnel. A modem modulates outgoing and

demodulates incoming carrier signals. These functions may coexist in one home router but remain conceptually distinct.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 13 | lines 78-83

Analog to Digital Conversion using modulation
The definition of the term modulation is described in the next section. Here we have modulation techniques:
• Pulse Amplitude Modulation (PAM)
• Pulse Code Modulation (PCM)
• Pulse Width Modulation (PWM)

Data Communication and Computer Networking module | PDF page 13 | lines 42-50

Digital Data to Digital Signal conversion
Coding methods are used to convert digital data into digital signals. There are two types of coding methods:
• Line Coding
• Block Coding
Scrambling is also one of the ways to convert digital data to digital signals but is not used.
Line Coding: It is the process of converting Digital data into digital signal.

Data Communication and Computer Networking module | PDF page 13 | lines 65-77

• Digital modulation is used to convert digital data to analog signal. Ex ASK, FSK, PSK.
Analog Modulation can be accomplished in three ways:
• Amplitude modulation (AM)
• Frequency modulation (FM)
• Phase modulation (PM).
Digital Modulation Types (Digital to Analog signal conversion)
Digital modulation is used to convert digital data to analog signal. It can be accomplished in the following ways:
• Amplitude Shift Keying(ASK)
• Frequency Shift keying (FSK)
• Phase Shift keying (PSK)

Question sources

Computer Science model exam · 2015 · Question 109

Question 58 | Q00647

In a peer-to-peer architecture, which statements are false? Select all that apply. Interpret C as absence of a required client-server hierarchy.

A. Computers can function as both a client and a server.

B. A dedicated central administrator is required by peer-to-peer architecture.

C. There is no a hierarchy among the computers.

D. In peer - to - peer network security is not an issue.

Hint

Use the cited note definitions to identify the requested function or scope, then check each alternative against that same rule.

Answer B, D: A dedicated central administrator is required by peer-to-peer architecture.; In peer - to - peer network security is not an issue.

Peers may request and supply services without a required client-server hierarchy. That capability does not impose a dedicated central administrator, although people may still take responsibility for administration. Peer systems also continue to need security because they expose data and services. The false statements therefore concern mandatory centralized administration and the dismissal of security, while the capability and no-required-hierarchy statements are true.

Why each choice is right or wrong

A - Incorrect: True: peers can both request and supply services, so this is not a false statement.

B - Correct: False: a dedicated central administrator is not a requirement of peer architecture.

C - Incorrect: True: peers do not require a client-server hierarchy, so this is not a false statement.

D - Correct: False: peer networks still require security.

Primary note proof

Study-note section NET02

> An intranet serves an organization internally; an extranet exposes selected services to approved outsiders. Neither term alone specifies geographic size. A client requests a service; a server supplies it. Peer systems may perform both roles. Dedicated servers concentrate on service workloads but can still be clients of DNS, backup or update services. A ten-user cutoff is a teaching guideline, not a technical law. Centralization simplifies administration but creates dependencies; peer networks still need security.

Study-note section NET33

> First identify the exact layer, protocol and scope. Flow/error control can exist at both link and transport layers; MAC addresses can be locally administered; bridges and switches both operate at layer 2. A LAN can use public or private unicast space. UDP and IP are both connectionless. Session dialogs and TCP connections are distinct senses of connection. Distinguish the protocol, layer and scope before treating these descriptions as exclusive.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 24 | lines 23-35

> Network Architecture: based on the architecture (where do the clients get the shared resources?), networks can be categorized into three:
> Client-Server Architecture: There can be one or more systems acting as Server. Other being Client, request the Server to serve requests. Servers take and process request on clients‘ behalf.
> Peer-to-Peer (Point-to-point): Two systems can be connected Point-to-Point, or in other words back-to-back fashion. They both reside on same level and called peers.
> There can be hybrid network which involves network architecture of both the above types.

Data Communication and Computer Networking module | PDF page 32 | lines 24-41

> A Windows workgroup is a group of standalone computers in a peer-to-peer network. Each computer in the workgroup uses its own local accounts database to authenticate resource access. The computers in a workgroup also do not have a common authentication process. The default-networking environment for a clean windows load is workgroup
> In general, a given Windows workgroup environment can contain many computers but work best with 15 or fewer computers. As the number of computers increases, a workgroup eventually become very difficult to administer and should be re-organized into multiple networks or set up as a client-server network.
> The computers in a workgroup are considered peers because they are all equal and share resources among each other without requiring a server. Since the workgroup doesn‘t share a common security and resource database, users and resources must be defined on each computer.

Question sources

Computer Science model exam · 2015 · Question 116

Question 59 | Q00653

Which of the following protocols uses both TCP and UDP?

A. FTP

B. SMTP

C. Telnet

D. DNS

Hint

Identify the requested service or delivery guarantee, then distinguish application roles, transport behavior and address configuration.

Answer D: DNS

Inspection of the module port table places DNS 53 in both TCP and UDP columns. The other named services occur only in its TCP column. Evidence: PDF 28, 18.

Why each choice is right or wrong

A - Incorrect: FTP 21 is listed in TCP only (PDF 28, 18.)

B - Incorrect: SMTP 25 is listed in TCP only (PDF 28, 18.)

C - Incorrect: Telnet 23 is listed in TCP only (PDF 28, 18.)

D - Correct: DNS 53 appears in both table columns (PDF 28, 18.)

Primary note proof

Study-note section NET20

> DNS resolves names to records, including IPv4 A and IPv6 AAAA addresses; it can use UDP or TCP port 53. DHCP dynamically leases IPv4 settings, commonly address, mask, gateway and DNS server. Its basic exchange is discover, offer, request, acknowledge. IP itself does not assign addresses.

Study-note section NET-S02

> In the conventional service bindings, FTP control, SMTP mail transfer and Telnet remote terminals use TCP. DNS supports both UDP and TCP on port 53; it is not exclusively a UDP service. The application protocol’s service role is distinct from the transport carrying its messages.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 28 | lines 23-31

> Telnet 23 SNMP 161
> SMTP 25 TFTP 69
> HTTP 80 DNS 53
> FTP 21 POP3 110
> DNS 53 DHCP 68

HTTPS 443 NTP 123
SSH 22 RPC 530
Table. Sample TCP and UDP port numbers from well-known category

Data Communication and Computer Networking module | PDF page 18 | lines 27-32

Application Layer
The Application Layer is a combination of Session, Presentation & Application Layers of OSI models and defines high level protocols like File Transfer (FTP), Electronic Mail (SMTP), Virtual Terminal (TELNET), Domain Name Service (DNS), etc.

Question sources

Computer Science model exam · 2015 · Question 122

Question 60 | Q00654

Which single option gives the complete set of listed devices whose ordinary forwarding function is at the data-link layer?

A. Switch

B. Access point

C. Hub

D. A & B

Hint

Match the requested scope or data unit to the layer duties in the note; distinguish hop delivery from end-to-end process delivery.

Answer D: A & B

An ordinary Ethernet switch forwards frames at layer 2, and an ordinary wireless access point bridges wireless and wired link-layer traffic. A hub simply repeats physical signals at layer 1. The question requests the complete set, so either switch or access point alone omits another qualifying device. The combined response is therefore the one complete selection.

Why each choice is right or wrong

A - Incorrect: A switch is layer 2, but this selection omits the qualifying access point.

B - Incorrect: A bridging access point is layer 2, but this selection omits the switch.

C - Incorrect: A hub repeats physical signals and does not inspect destination MAC addresses as a data-link device does.

D - Correct: Both the ordinary switch and bridging access point are data-link devices; this gives the complete set.

Primary note proof

Study-note section NET10

A bridge or ordinary Ethernet switch operates at layer 2. It learns source-MAC-to-port mappings, looks up the destination, forwards a known unicast to its port, filters it if the destination is on the incoming segment, and floods an unknown unicast or broadcast within its VLAN. A switch does not always send only to one destination port. Wireless access points normally bridge wireless and wired link-layer traffic.

Study-note section NET09

A repeater regenerates layer-1 signals without inspecting destination addresses. An active hub is a multiport repeater: it repeats incoming signals onto other ports, placing half-duplex endpoints in one collision domain. A passive hub is a connector. A hub neither learns MAC addresses nor eliminates collisions. An endpoint such as a network printer consumes services; routers, hubs and access points are intermediary devices.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 12 | lines 27-37

SWITCH: A switch filters and forwards data packets
across anetwork.
Unlike a hub which simply replicates what it receives on
oneport onto all the other ports, a switch keeps a record
of the MAC addresses of the devices attached to it.
When the switch receives a data packet, it forwards the
packetdirectly to the recipient device by looking up the
MAC address.
• Switch is intelligent and expensive than Hub
• Switch is a point to point communication device
• Hub is a broadcasting device

Data Communication and Computer Networking module | PDF page 12 | lines 17-26

Active Hubs
An active hub is actually a multipart repeater. It is
normallyused to create connections between stations in
a physical startopology.
HUB: Hubs are commonly used to connect segments
(devices)of a LAN. Hubs don‘t filter information; instead
broadcast incoming packets to all computers connected to
it. A hub contains multiple ports which support 8, 12 or
24 RJ-45 ports. Two types: Passive hub and Active hub. It
is used in star or ring topology.

Data Communication and Computer Networking module | PDF page 15 | lines 13-40

Data Link Layer
• The Data Link layer adds reliability to the physical

layer by providing error detection and correction mechanisms.
• Framing: the Data Link layer receives the data from Network Layer and divides the stream of bits into fixed size manageable units called as Frames and sends it to the physical layer. On the receiver side, the data link layer receives the stream of bits from the physical layer and regroups them into frames and sends them to the Network layer.
• Physical Addressing: The Data link layer appends the physical address in the header of the frame before sending it to physical layer.
• Flow control: The data link layer makes sure that the sender sends the data at a speed at which the receiver canreceive it else if there is an overflow at the receiver sidethe data will be lost.
• Error Control: The data link layer imposes error control mechanism to identify lost or damaged frames, duplicateframes and then retransmit them.
• Access Control: The data link layer imposes access control mechanism to determine which device has right to send data in an multipoint connection setting.
• Main Responsibility: The main responsibility of the data link layer is hop to hop transmission of frames.

Question sources

Computer Science model exam · 2015 · Question 123

Question 61 | Q00656

Which statement correctly describes the OSI reference model?

A. It has fewer layer that TCP/IP model.

B. The model itself is executable software installed to implement a network.

C. Used as a guide to help students or learners understand the communication process.

D. All

Hint

Match the requested scope or data unit to the layer duties in the note; distinguish hop delivery from end-to-end process delivery.

Answer C: Used as a guide to help students or learners understand the communication process.

OSI divides communication responsibilities into seven layers and serves as a framework for explaining interfaces and communication processes. The usual TCP/IP teaching model has four layers, so OSI does not have fewer. A reference model can guide design, but it is not itself executable networking software or an installed protocol implementation. That distinction makes the learning-guide statement the correct description.

Why each choice is right or wrong

A - Incorrect: OSI has seven layers, more than the usual four-layer TCP/IP teaching model.

B - Incorrect: A reference model is not itself executable networking software, although it can guide design.

C - Correct: The model helps learners understand layered communication responsibilities.

D - Incorrect: The incorrect layer count and executable-software claim prevent all statements from being true.

Primary note proof

Study-note section NET03

> A reference model divides responsibilities and interfaces; it is not itself executable networking software. OSI is a seven-layer reference model; TCP/IP describes an implemented protocol suite, usually taught with four layers. A five-layer teaching model separates physical and link functions. State the model before counting layers.

Study-note section NET19

> The four-layer TCP/IP model folds OSI layers 5-7 into application, retains transport, calls layer 3 Internet, and combines link/physical as network access. A model is a guide to functions, not a guarantee that every application gets a reliable network. Distinguish end-to-end application service from its underlying process-to-process transport.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 14 | lines 12-29

> The Open Systems Interconnection (OSI) Model was
> developed by International Organization for Standardization
> (ISO). ISO is the organization, OSI is the model
> It was developed to allow systems with different platforms
> (Hardware & software) to communicate with each other.
> Now, it is a network model that defines the protocols for
> network communications.
> It is a hierarchical model that groups its processes into seven
> (7) layers. (Top to Bottom)
> 1. Application Layer
> 2. Presentation Layer

3. Session Layer
4. Transport Layer
5. Network Layer
6. Data Link Layer
7. Physical Layer
Each layer has specific functions to perform and has to co-operate with the layers above and below it.

Data Communication and Computer Networking module | PDF page 17 | lines 3-15

The structure TCP/IP model is very similar to the structure of the OSI reference model. The OSI model has seven layers where the TCP/IP model has four layers.
• The Application layer of TCP/IP model corresponds to the Application Layer of Session, Presentation & Application Layer of OSI model.
• The Transport layer of TCP/IP model corresponds to theTransport Layer of OSI model
• The Network layer of TCP/IP model corresponds to the Network Layer of OSI model
• The Host to network layer of TCP/IP model correspondsto the Physical and Data link Layer of OSI model.

Data Communication and Computer Networking module | PDF page 25 | lines 17-27

TCP/IP is a hierarchical protocol made up of interactive modules, each of which provides a specific functionality; however, the modules are not necessarily interdependent. Whereas the OSI model specifies which functions belong to each of its layers, the layers of TCP/IP suite contain relatively independent protocols that can be mixed and matched depending on the needs of the system. The term hierarchical means that each upper-level protocol is supported by one or more lower-level protocols.

Question sources

Computer Science model exam · 2015 · Question 125

Question 62 | Q00699

Which listed item is not one of the five basic components of data communication?

A. Message

B. Medium

C. Sender

D. Distance

Hint

Use the cited note definitions to identify the requested function or scope, then check each alternative against that same rule.

Answer D: Distance

The five basic components are message, sender, receiver, medium and protocol. Message, medium and sender therefore belong to the required set. Distance affects transmission engineering, such as propagation delay and attenuation, but it is not a sixth component in that model. Replacing the original protocol option with distance supplies a meaningful exception while retaining the negative component-identification task.

Why each choice is right or wrong

A - Incorrect: Message is explicitly one of the required components.

B - Incorrect: The medium carries signals and is explicitly a communication component.

C - Incorrect: The sender is explicitly included among communication components.

D - Correct: Distance affects engineering but is not one of the five basic communication components.

Primary note proof

Study-note section NET01

> Data are raw representations; information is data interpreted for a purpose. Communication requires a message, sender, receiver, medium and agreed protocol. A source creates data; a transmitter converts it to a signal; a receiver reconstructs data. Distance affects engineering but is not a sixth component.

Study-note section NET06

> Transmission delay is packet bits divided by link bit rate; propagation delay is distance divided by signal speed. Processing and queueing add delay. A 1000-byte packet takes 0.8 ms to serialize at 10 Mbit/s; increasing line rate does not reduce propagation time.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 5 | lines 23-35

A Data Communication system has five components:-
• Message:- is the information to be communicated by the sender to the receiver.
• Sender The sender is any device that is capable of sending the data (message).
• Receiver: - is a device that the sender wants to communicate the data (message).
• Transmission Medium: - It is the path by which the message travels from sender to receiver. It can be wired or wireless and many subtypes in both.
• Protocol:- It is an agreed upon set or rules used by the sender and receiver to communicate data. Rules that govern data communication.

Question sources

Computer Science model exam 2 · Question 40

Question 63 | Q00700

There are two types of network topologies from these topologies which one of the following defines how hosts access the media to send data.

A. Logical Topology

B. Bus Topology

C. Physical Topology

D. Star Topology

Hint

Draw the links and identify shared components, alternate paths and the effect of the specified failure or growth requirement.

Answer A: Logical topology

The distinction is between physical layout and communication/access relationships. NET08 defines logical topology in the latter sense, matching how hosts obtain medium access. Bus and star are particular arrangements rather than the general physical-versus-logical category requested.

Why each choice is right or wrong

A - Correct: Logical topology describes communication and medium-access relationships among hosts.

B - Incorrect: Bus is a particular shared-backbone arrangement, not the general category defining access relationships.

C - Incorrect: Physical topology describes link layout and connections rather than the logical rules for medium access.

D - Incorrect: Star describes endpoints around a central device; it does not name the general access-topology category.

Primary note proof

Study-note section NET08

Physical topology describes link layout; logical topology describes communication/access relationships. Point-to-point links join two endpoints; multipoint links share a medium. A full mesh consists of point-to-point links.

Study-note section NET08

Bus uses a shared backbone; an unterminated break can disrupt the segment. Star connects endpoints through a central device: one edge failure isolates that endpoint, whereas central failure affects the star. Ring forms a loop; basic single rings are vulnerable to a break, while protected dual rings differ. Token passing is associated with Token Ring but is an access method, not a necessary property of every ring. Tree is hierarchical; hybrid combines arrangements.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 11 | lines 34-51

NETWORK TOPOLOGY
A network topology is a description of the layout of the region or area covered by that network.
There are two types of connections. They are: point-to-point and multi-point.
Point-to-point connections provide a direct link between two devices.
Multi-point connections provide a link between three or more devices on a network.
There are seven basic topologies in the study of network topology:
• Point-to-point topology,
• Bus (point-to-multipoint) topology,
• Ring topology,
• Star topology,
• Hybrid topology,
• Mesh topology and,
• Tree topology.

Data Communication and Computer Networking module | PDF page 22 | lines 45-52

Inter-connectivity: components of a network, including end devices and interconnecting devices, can be connected to each other differently in some fashion. By connectedness we mean either logically, physically or both ways. Network topology refers to the shape of a network, or the network‘s layout. It is

the geometric representation of the relationship of all
the links and linking devices to one another. There are

Question sources

Computer Science model exam 2 · Question 41

Question 64 | Q00701

Segmentation of a data stream happens at which layer of the OSI model?

A. Physical

B. Data Link

C. Network

D. Transport

Hint

Match the requested scope or data unit to the layer duties in the note; distinguish hop delivery from end-to-end process delivery.

Answer D: Transport

Transport explicitly divides data into segments and reassembles sequence-numbered segments. Evidence: PDF 16, 14, 15, 15.

Why each choice is right or wrong

A - Incorrect: Physical delivers bits (PDF 16, 14, 15, 15.)

B - Incorrect: Data link handles frames (PDF 16, 14, 15, 15.)

C - Incorrect: Network handles packets (PDF 16, 14, 15, 15.)

D - Correct: Transport explicitly performs segmentation (PDF 16, 14, 15, 15.)

Primary note proof

Study-note section NET12

Sending proceeds from application data to transport segment/datagram, network packet, link frame and physical bits/symbols; receiving reverses the order. Each layer serves the layer above. A router removes a received link frame, inspects IP, and creates a new link frame for the next hop. MAC addresses usually change across routed hops; end-to-end IP addresses ordinarily remain until translation.

Study-note section NET17

TCP offers a reliable ordered byte stream using sequence numbers, acknowledgments, retransmission and windows. Flow control protects the receiver; congestion control protects network capacity. UDP sends independent datagrams with ports and a checksum but no built-in

setup, delivery guarantee, retransmission or ordering. Live interactive traffic may choose UDP when late data is less useful than lost data. Application protocols can add reliability over UDP.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 16 | lines 2-17

• At the sending side, the transport layer receives data from the session layer, divides it into units called segments and sends it to the network layer.
• To ensure process to process delivery the transport layer makes use of port address to identify the data from the sending and receiving process.
• The data can be transported in a connection oriented or connectionless manner.
• The Transport layer is responsible for segmentation and reassembly of the message into segments which bear sequence numbers.
• The transport layer also carries out flow control and error control functions; but unlike data link layer these are end to end rather than node to node.
• The main responsibility of the transport layer is process to process delivery of the entire message

Data Communication and Computer Networking module | PDF page 14 | lines 32-49

Physical Layer:
• The Physical Layer provides a standardized interface to physical transmission media, including: Mechanical specification of electrical connectors and cables, for example maximum cable length, Electrical specification of transmission line and Bit-by-bit or symbol-by-symbol delivery.
• Interface: The Physical Layer defines the characteristics of interfaces between the devices & transmission medium.
• Representation of bits: The physical layer is concerned with transmission of signals from one device to another which involves converting data (1_s & 0_s) into signals and vice versa. It is not concerned with the meaning or interpretation of bits.
• Data rate: The physical layer defines the data transmission rate i.e. number of bits sent per second. It is the responsibility of the physical layer to maintain the defined data rate.

Data Communication and Computer Networking module | PDF page 15 | lines 13-40

Data Link Layer
• The Data Link layer adds reliability to the physical

layer by providing error detection and correction mechanisms.
• Framing: the Data Link layer receives the data from Network Layer and divides the stream of bits into fixed size manageable units called as Frames and sends it to the physical layer. On the receiver side, the data link layer receives the stream of bits from the physical layer and regroups them into frames and sends them to the Network layer.
• Physical Addressing: The Data link layer appends the physical address in the header of the frame before sending it to physical layer.
• Flow control: The data link layer makes sure that the sender sends the data at a speed at which the receiver canreceive it else if there is an overflow at the receiver sidethe data will be lost.
• Error Control: The data link layer imposes error control mechanism to identify lost or damaged frames, duplicateframes and then retransmit them.
• Access Control: The data link layer imposes access control mechanism to determine which device has right to send data in an multipoint connection setting.
• Main Responsibility: The main responsibility of the data link layer is hop to hop transmission of frames.

Data Communication and Computer Networking module | PDF page 15 | lines 41-61

Network Layer
• The network layer makes sure that the data is deliveredto the receiver despite multiple intermediate devices.
• The network layer at the sending side accepts data from the transport layer, divides it into packets, addsaddressing information in the header and passes it tothe data link layer.
• The network layer is responsible for source todestination of delivery of data.
• The network layer uses logical address commonlyknown as IP address to recognize devices on the network.
• Each packet is independent of the other and may travelusing different routes to reach the receiver hence may arrive out of turn at the receiver (Routing).
• The Network layer does not perform any flow

controlor error control
• The main responsibility of Network Layer is
transmission of packets from source to destination

Question sources

Computer Science model exam 2 · Question 42

Question 65 | Q00702

When data is encapsulated, which is the correct order?

A. Data, frame, packet, segment, bit

B. Data, segment, packet, frame, bit

C. Segment, data, packet, frame, bit

D. Data, segment, frame, packet, bit

Hint

Match the requested scope or data unit to the layer duties in the note; distinguish hop delivery from end-to-end process delivery.

Answer B: Data, segment, packet, frame, bit

Follow the sending path downward: upper data becomes transport segments, network packets, data-link frames, then physical bits. Evidence: PDF 16, 15, 15, 14.

Why each choice is right or wrong

A - Incorrect: Frames cannot precede network packets on the sending path

B - Correct: The encapsulation order is data, segment, packet, frame, then bit

C - Incorrect: Segmentation follows receipt of upper-layer data

D - Incorrect: Network packet must precede data-link frame

Primary note proof

Study-note section NET12

Sending proceeds from application data to transport segment/datagram, network packet, link frame and physical bits/symbols; receiving reverses the order. Each layer serves the layer above. A router removes a received link frame, inspects IP, and creates a new link frame for the next hop. MAC addresses usually change across routed hops; end-to-end IP addresses ordinarily remain until translation.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 16 | lines 2-17

• At the sending side, the transport layer receives data from the session layer, divides it into units called segments and sends it to the network layer.
• To ensure process to process delivery the transport layer makes use of port address to identify the data from the sending and receiving process.
• The data can be transported in a connection oriented or connectionless manner.
• The Transport layer is responsible for segmentation and reassembly of the message into segments which bear sequence numbers.
• The transport layer also carries out flow control and error control functions; but unlike data link layer these are end to end rather than node to node.
• The main responsibility of the transport layer is process to process delivery of the entire message

Data Communication and Computer Networking module | PDF page 15 | lines 41-61

Network Layer
• The network layer makes sure that the data is deliveredto the receiver despite multiple intermediate devices.
• The network layer at the sending side accepts data from the transport layer, divides it into packets, addsaddressing information in the header and passes it tothe data link layer.
• The network layer is responsible for source todestination of delivery of data.
• The network layer uses logical address commonlyknown as IP address to recognize devices on the network.
• Each packet is independent of the other and may travelusing different routes to reach the receiver hence may arrive out of turn at the receiver (Routing).
• The Network layer does not perform any flow controlor error control
• The main responsibility of Network Layer is transmission of packets from source to destination

Data Communication and Computer Networking module | PDF page 15 | lines 13-40

Data Link Layer
• The Data Link layer adds reliability to the physical layer by providing error detection and correction mechanisms.
• Framing: the Data Link layer receives the data from Network Layer and divides the stream of bits

into fixed size manageable units called as Frames and sends it to the physical layer. On the receiver side, the data link layer receives the stream of bits from the physical layer and regroups them into frames and sends them to the Network layer.
• Physical Addressing: The Data link layer appends the physical address in the header of the frame before sending it to physical layer.
• Flow control: The data link layer makes sure that the sender sends the data at a speed at which the receiver canreceive it else if there is an overflow at the receiver sidethe data will be lost.
• Error Control: The data link layer imposes error control mechanism to identify lost or damaged frames, duplicateframes and then retransmit them.
• Access Control: The data link layer imposes access control mechanism to determine which device has right to send data in an multipoint connection setting.
• Main Responsibility: The main responsibility of the data link layer is hop to hop transmission of frames.

Data Communication and Computer Networking module | PDF page 14 | lines 32-49

Physical Layer:
• The Physical Layer provides a standardized interface to physical transmission media, including: Mechanical specification of electrical connectors and cables, for example maximum cable length, Electrical specification of transmission line and Bit-by-bit or symbol-by-symbol delivery.
• Interface: The Physical Layer defines the characteristics of interfaces between the devices & transmission medium.
• Representation of bits: The physical layer is concerned with transmission of signals from one device to another which involves converting data (1_s & 0_s) into signals and vice versa. It is not concerned with the meaning or interpretation of bits.
• Data rate: The physical layer defines the data transmission rate i.e. number of bits sent per second. It is the responsibility of the physical layer to maintain the defined data rate.

Question sources

Computer Science model exam 2 · Question 43

Question 66 | Q00703

You want to implement a network medium that is not susceptible to EMI. Which type of cabling should you use?

A. Coaxial

B. Category 6 UTP

C. Microwave

D. Fiber-optic

Hint

Compare the signal mechanism, medium properties or transmission direction against the definitions and stated physical assumptions.

Answer D: Fiber-optic cable

NET07 identifies fiber as a light-guiding medium that resists electromagnetic interference. Coax and UTP carry electrical signals and can be affected by coupled interference. Microwave is wireless, so it is not a cabling answer even before considering interference in radio transmission.

Why each choice is right or wrong

A - Incorrect: Coax has shielding but still carries electrical signals; it does not offer fiber's immunity to electromagnetic coupling.

B - Incorrect: Twisted pairs reduce interference but unshielded copper cable remains susceptible to electromagnetic coupling.

C - Incorrect: Microwave is an unguided wireless medium, not a cable matching the requested cabling choice.

D - Correct: Fiber carries light and resists electromagnetic interference rather than conducting the unwanted electrical coupling.

Primary note proof

Study-note section NET07

> Twisted pairs reduce coupled interference; UTP has no added shield and STP adds shielding. Coax has an inner conductor and outer shield sharing an axis. Fiber guides light and resists electromagnetic interference; it supports high capacity and long reach, but requires suitable optics and installation. Exact speed, cost and reach depend on the specification, not the material alone. Fiber can still be tapped.

Study-note section NET07

> Radio, microwave and infrared are unguided media. Ground waves follow Earth, sky waves can reflect from ionized layers, and line-of-sight paths require suitable visibility. Microwaves are radio waves in the broader physical classification. Infrared generally does not penetrate walls. Directionality depends on antennas: omnidirectional means broad azimuth coverage, not equal radiation in every 3-D direction. Legacy Ethernet straight-through cables join unlike MDI/MDI-X

roles; crossover joins like roles, such as PC-PC or switch-switch. Auto-MDI-X can remove that requirement.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 10 | lines 36-55

TRANSMISSION MEDIA
Transmission media is a means by which a communicationsignal is carried from one system to another
A transmission medium can be defined as anything that cancarry information from a source to a destination. The transmission medium is usually free space, metallic cable orfiber optic cable. Guided and Unguided (WIRELESS) Guided Transmission Media uses a cabling system that guidesthe data signals along a specific path. Out of these twisted-paircable, coaxial cable transport signals in the form of electricsignals and fiber-optic cable transport signals in the form oflight.
Unguided Transmission Media transport data without using a physical conductor. It uses wireless electromagnetic signals to send data. Three types of unguided media:
• Radio waves
• Micro waves
• Infrared.

Data Communication and Computer Networking module | PDF page 11 | lines 23-33

Twisted-pair cable: Consists of two conductors (normally copper), each with its own plastic insulation, twisted together.
Two types
• Unshielded Twisted-Pair cable (UTP)
• Shielded Twisted-Pair cable (STP)
Coaxial cable:- uses copper wire to conduct the signals electronically
Fiber-optic cable:- uses glass or plastic conductor and transmits the signals as light
Wireless/Unguided media the signal propagates in the atmosphere and in outer space

Question sources

Computer Science model exam 2 · Question 44

Question 67 | Q00704

Which responsibility belongs to the OSI network layer rather than the data-link layer?

A. logical link control

B. Network Addressing

C. media access control

D. Hardware Addressing

Hint

Match the requested scope or data unit to the layer duties in the note; distinguish hop delivery from end-to-end process delivery.

Answer B: Network Addressing

Logical network addressing, such as IP addressing, supports delivery across interconnected networks and belongs to the network layer. The data-link layer instead handles local frame delivery, hardware/MAC addressing, medium access and link-control functions. LLC identifies or multiplexes upper-layer protocols and may supply link control. The term hardware addressing here denotes frame-level MAC addressing, not an IP address.

Why each choice is right or wrong

A - Incorrect: LLC is a data-link sublayer role for upper-protocol identification and link control.

B - Correct: Logical network addressing is a network-layer responsibility.

C - Incorrect: Medium access control is a data-link role.

D - Incorrect: MAC hardware addressing is used for link-frame delivery.

Primary note proof

Study-note section NET13

> Link-layer LLC identifies or multiplexes upper-layer protocols and may supply link control; MAC handles medium-dependent addressing/access and frame delivery. Network addressing belongs to layer 3. Ethernet, PPP and HDLC are link protocols. Frame headers may carry addresses and control/type fields; synchronization and exact framing depend on the protocol.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 15 | lines 13-40

> Data Link Layer
> • The Data Link layer adds reliability to the physical layer by providing error detection and correction mechanisms.
> • Framing: the Data Link layer receives the data from Network Layer and divides the stream of bits into fixed size manageable units called as Frames

and sends it to the physical layer. On the receiver side, the data link layer receives the stream of bits from the physical layer and regroups them into frames and sends them to the Network layer.
• Physical Addressing: The Data link layer appends the physical address in the header of the frame before sending it to physical layer.
• Flow control: The data link layer makes sure that the sender sends the data at a speed at which the receiver canreceive it else if there is an overflow at the receiver sidethe data will be lost.
• Error Control: The data link layer imposes error control mechanism to identify lost or damaged frames, duplicateframes and then retransmit them.
• Access Control: The data link layer imposes access control mechanism to determine which device has right to send data in an multipoint connection setting.
• Main Responsibility: The main responsibility of the data link layer is hop to hop transmission of frames.

Data Communication and Computer Networking module | PDF page 15 | lines 41-61

Network Layer
• The network layer makes sure that the data is deliveredto the receiver despite multiple intermediate devices.
• The network layer at the sending side accepts data from the transport layer, divides it into packets, addsaddressing information in the header and passes it tothe data link layer.
• The network layer is responsible for source todestination of delivery of data.
• The network layer uses logical address commonlyknown as IP address to recognize devices on the network.
• Each packet is independent of the other and may travelusing different routes to reach the receiver hence may arrive out of turn at the receiver (Routing).
• The Network layer does not perform any flow controlor error control
• The main responsibility of Network Layer is transmission of packets from source to destination

Question sources

Computer Science model exam 2 · Question 45

Question 68 | Q00705

Which class of IP address provides a maximum of only 254 host addresses per network ID?

A. Class A

B. Class D

C. Class B

D. Class C

Hint

Convert the mask to a prefix, separate network and host bits, and apply the relevant subnet-count or usable-host rule.

Answer D: Class C under the historical default mask

The wording asks about historical address classes. Class C uses default /24, leaving eight host bits: 2^8−2=254 ordinary usable hosts. Classes A and B leave more bits, while Class D identifies multicast rather than an ordinary unicast host network. Under CIDR the actual prefix would replace these defaults.

Why each choice is right or wrong

A - Incorrect: Default Class A /8 leaves 24 host bits, far more than 254 usable hosts.

B - Incorrect: Class D is multicast space, not an ordinary classful unicast network with 254 hosts.

C - Incorrect: Default Class B /16 leaves sixteen host bits and 65534 ordinary usable hosts.

D - Correct: Default Class C /24 leaves eight host bits, giving 256 addresses minus network and broadcast.

Primary note proof

Study-note section NET22

> Historical classes use leading patterns: A 0 with /8, B 10 with /16, C 110 with /24; D 1110 is multicast and E 1111 reserved. Ordinary class-A first octets are 1-126 because 0 and 127 have special uses. B spans 128-191 and C 192-223. Default usable counts are 2^24-2, 2^16-2 and 254. Modern CIDR requires the actual prefix and overrides class defaults.

Study-note section NET25

> For ordinary broadcast LANs let h=32-p. Total addresses=2^h; usable hosts=2^h-2, reserving network and directed broadcast. Find the changing octet’s increment as 256-mask octet, round the address down to a multiple, and extend through the next boundary minus one.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 19 | lines 37-44

CIDR: A class B address is far too large for most organizationsand a class C network, with 256 addresses is too small. This leads to granting Class B address to organizations who do not require all. This is resulting in depletion of Address space. A solution is CIDR (Classless InterDomain Routing) The basic idea behind CIDR, is to allocate the remaining IP addresses in variable-sized blocks, without regard to the classes.

Data Communication and Computer Networking module | PDF page 19 | lines 2-22

Address Space: An address space is the total number ofaddresses used by the protocol.
• If a protocol uses N bits to define an address, the address space is 2N because each bit can have twodifferent values (0 or 1) and N bits can have 2N values.
• IPv4 uses 32-bit addresses, which means that the address space is 232 or 4,294,967,296 (more than 4billion).
Notations: There are two notations to show an IPv4 address:
• Binary notation: The IPv4 address is displayed as 32bits. ex. 11000001 10000011 00011011 11111111
• Dotted decimal notation: To make the IPv4 address easier to read, Internet addresses are usually written in decimal form with a decimal point (dot) separatingthe bytes. Each byte (octet) is 8 bits hence each number in dotted-decimal notation is a value rangingfrom 0 to 255. Ex. 129.11.11.239

Data Communication and Computer Networking module | PDF page 19 | lines 23-36

Classful addressing : In classful addressing, the addressspace is divided into five classes: A, B, C, D, and E.
• Netid and Hostid In classful addressing, an IP addressin class A, B, or C is divided into netid and hostid.
Subnetting: It allows a network to be split into several parts for internal use but still act like a single network to the outsideworld.
• To implement subnetting, the router needs a

subnet mask that indicates the split between network + subnet number and host. Ex. 255.255.252.0/22. A‖/22‖ to indicate that the subnet mask is 22 bits long.

Question sources

Computer Science model exam 2 · Question 46

Question 69 | Q00706

Which item is not a parameter or spatial characteristic of a continuous sinusoidal carrier wave?

A. Amplitude

B. Wavelength

C. phase

D. Discrete pulse

Hint

Compare the signal mechanism, medium properties or transmission direction against the definitions and stated physical assumptions.

Answer D: Discrete pulse

A sine wave has amplitude, frequency and phase. Given propagation speed, wavelength follows from frequency and describes its spatial repetition. A discrete pulse is a different waveform description, not a parameter of a continuous sine wave. This distinction concerns the specified carrier model; it does not claim that all pulse modulation is digital, since pulse amplitude and width can vary to carry analog information.

Why each choice is right or wrong

A - Incorrect: Amplitude specifies the sinusoid’s magnitude.

B - Incorrect: Wavelength specifies the spatial repetition of the propagating sinusoid.

C - Incorrect: Phase specifies displacement within the sinusoid’s cycle.

D - Correct: A discrete pulse is a waveform description rather than a sinusoidal parameter.

Primary note proof

Study-note section NET04

Analog signals vary continuously; digital signals use discrete symbol states. Data and signal types are separate: digital bits can modulate an analog carrier. A sine wave has amplitude, frequency and phase. Frequency f counts cycles/second, period T=1/f, and wavelength λ=v/f depends on propagation speed v. Phase specifies displacement within a cycle. Composite signals combine frequencies.

Study-note section NET15

Line coding maps digital bits to digital signal patterns. NRZ uses levels without a forced mid-bit return; Manchester supplies a mid-bit transition for clocking, with bit convention specified. Differential Manchester encodes using transitions relative to previous state. AMI alternates the polarity of successive ones; pseudoternary alternates zero pulses. Block coding adds code redundancy; scrambling replaces problematic patterns without necessarily increasing bit count. Multilevel schemes include 2B1Q and 8B6T; MLT-3 uses a sequence of voltage transitions.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 7 | lines 40-48

ANALOG SIGNAL
An analog signal has infinitely many levels of intensity over a period of time.
A simple analog signal is a sine wave that cannot be further decomposed into simpler signals.
A sine wave is characterized by three parameters:
• Peak Amplitude
• Frequency
• Phase

Data Communication and Computer Networking module | PDF page 7 | lines 73-82

Wavelength
The wavelength of a signal refers to the relationship between frequency (or period) and propagation speed of the wave through a medium.
The wavelength is the distance a signal travels in one period.
It is given by
Wavelength = Propagation Speed X Period
OR
Wavelength =Propagation Speed X 1/Frequency

Data Communication and Computer Networking module | PDF page 7 | lines 89-94

DIGITAL SIGNAL
Digital Signal: Information can also be explained in the form of a digital signal. A digital signal can be explained with the help of following points:
A digital is a signal that has discrete values.
The signal will have value that is not continuous.

Question sources

Computer Science model exam 2 · Question 47

Question 70 | Q00707

Communication between a radio station and its listeners involves _____ transmission.

A. full-duplex

B. Half-duplex

C. Simplex

D. Automatic

Hint

Use the cited note definitions to identify the requested function or scope, then check each alternative against that same rule.

Answer C: Simplex

An ordinary broadcast radio station transmits to listeners who only receive. The one-direction relationship matches simplex. Evidence: PDF 5.

Why each choice is right or wrong

A - Incorrect: Full duplex requires both sides simultaneously transmitting (PDF 5.)

B - Incorrect: Half duplex requires alternate two-way transmission (PDF 5.)

C - Correct: Simplex explicitly has one sender and one receiver direction (PDF 5.)

D - Incorrect: Automatic is not one of the module transmission modes (PDF 5.)

Primary note proof

Study-note section NET06

> Simplex is one way, half duplex alternates directions, and full duplex permits simultaneous sending/receiving. A walkie-talkie is half duplex; a telephone conversation uses full duplex. Serial sends sequential bits; parallel uses multiple conductors and may suffer skew. Character-oriented asynchronous serial adds start/stop bits; synchronous framing uses ongoing clock recovery. Neither is synonymous with browser asynchronous requests.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 5 | lines 43-48

> • Simplex: Only one of the devices sends the data and the other one only receives the data (Unidirectional).
> • Half Duplex: both the stations can transmit as well as receive but not at the same time.
> • Full duplex mode: both stations can transmit and receive at the same time.

Question sources

Computer Science model exam 2 · Question 48

Question 71 | Q00708

Which of the following does not describe router functions

A. Broadcast forwarding

B. Internetwork communication

C. Packet filtering

D. Packet switching

Hint

Compare signal repetition, frame forwarding, packet routing and policy enforcement using the stated device or traffic assumptions.

Answer A: Forwarding local broadcasts is not a normal router function

Routers forward IP packets between networks and separate broadcast domains. Accordingly internetwork communication and packet forwarding/switching describe routing, whereas ordinary local link broadcasts are not propagated across routers. Packet filtering can accompany the traffic-control function, so A is the normal-function exception, not a claim that no specially configured broadcast relay can exist.

Why each choice is right or wrong

A - Correct: Ordinary routers bound broadcast domains rather than forwarding local link broadcasts between them.

B - Incorrect: Forwarding IP packets between different networks is the defining router function.

C - Incorrect: Traffic filtering can be implemented alongside routing; it is consistent with router security-policy controls.

D - Incorrect: A router forwards individual packets to next hops, a network-layer packet-switching function.

Primary note proof

Study-note section NET11

> Routers forward IP packets between networks using destination prefixes and next hops. They separate broadcast domains and normally do not forward local link broadcasts. A default gateway is usually a router, while a protocol gateway can translate application formats; therefore a gateway is not inherently a device that implements every OSI layer.

Study-note section NET11

> A firewall allows, rejects or inspects traffic under a security policy; it does not necessarily encrypt. A VPN, Virtual Private Network, provides a logical private connection over another network; a secure VPN authenticates/encrypts its tunnel. A modem modulates outgoing and

demodulates incoming carrier signals. These functions may coexist in one home router but remain conceptually distinct.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 12 | lines 38-52

ROUTER: Router is a specialized network device
used tointerconnect different types of network that
uses different protocol.
Router allows the users to connect several LAN and WAN
• A LAN to another LAN
• A WAN to another WAN
• A LAN to the Internet
Routers use the routing table to determine how to
forwardpackets.
• The list of routing tables provides directions to
transfer the data to a particular network
destination -various paths to forward the data.
• A router analyzes a destination IP address of a
givenpacket and compares it with the routing
table to decide the packet's next best path

Data Communication and Computer Networking module | PDF page 48 | lines 29-40

Network Address Translation (NAT)
NAT translates the IP addresses of computers in a local network to a single IP address. This address is often used by the router that connects the computers to the Internet. The router can be connected to a DSL modem, cable modem, T1 line, or even a dial-up modem. When other computers on the Internet attempt to access computers within the local network, they only see the IP address of the router. This adds an extra level of security, since the router can be configured as a firewall, only allowing authorized systems to access the computers within the network.

Data Communication and Computer Networking module | PDF page 13 | lines 2-8

Filters content by reading the MAC addresses of source and
destination.
• MAC to Segment number table
• Do not filter broadcast
• Data not destined for other network is prevented from
passing over the bridge
• Slower than repeater due to filtering

Question sources

Computer Science model exam 2 · Question 49

Question 72 | Q00709

Which OSI layer uses acknowledgments, sequencing and receiver flow control for end-to-end process delivery, as illustrated by TCP?

A. Layer 2

B. Layer 4

C. Layer 3

D. Layer 7

Hint

Match the requested scope or data unit to the layer duties in the note; distinguish hop delivery from end-to-end process delivery.

Answer B: Layer 4

Scope separates otherwise similar mechanisms. Reliable link procedures can acknowledge frames and control a single hop, whereas TCP uses sequence numbers, acknowledgments and windows between transport endpoints. The explicit end-to-end process-delivery requirement identifies layer 4. IP at layer 3 offers best-effort delivery, and application services build on the transport service rather than defining this TCP reliability machinery.

Why each choice is right or wrong

A - Incorrect: Layer 2 can provide similar mechanisms only for hop-local link delivery, outside the requested scope.

B - Correct: Layer 4 transport provides TCP’s end-to-end sequencing, acknowledgments and receiver flow control.

C - Incorrect: IP best-effort delivery does not provide the indicated ordered acknowledgment/retransmission service.

D - Incorrect: Application services can build reliability, but the standard link/transport mechanisms named here are not layer-7 duties.

Primary note proof

Study-note section NET14

> Controlled access uses polling, reservations or a token to grant turns; correctly coordinated access avoids contention collisions. Channelization divides frequency, time or code resources. Stop-and-wait sends one frame and waits for ACK, retransmitting on timeout; sequence bits distinguish duplicates. Sliding windows permit multiple unacknowledged frames. Link reliability/flow control is hop-local; transport reliability/flow control is end-to-end. Ethernet detects corruption but does not itself guarantee reliable delivery.

Study-note section NET17

TCP offers a reliable ordered byte stream using sequence numbers, acknowledgments, retransmission and windows. Flow control protects the receiver; congestion control protects network capacity. UDP sends independent datagrams with ports and a checksum but no built-in setup, delivery guarantee, retransmission or ordering. Live interactive traffic may choose UDP when late data is less useful than lost data. Application protocols can add reliability over UDP.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 15 | lines 13-40

Data Link Layer
• The Data Link layer adds reliability to the physical layer by providing error detection and correction mechanisms.
• Framing: the Data Link layer receives the data from Network Layer and divides the stream of bits into fixed size manageable units called as Frames and sends it to the physical layer. On the receiver side, the data link layer receives the stream of bits from the physical layer and regroups them into frames and sends them to the Network layer.
• Physical Addressing: The Data link layer appends the physical address in the header of the frame before sending it to physical layer.
• Flow control: The data link layer makes sure that the sender sends the data at a speed at which the receiver canreceive it else if there is an overflow at the receiver sidethe data will be lost.
• Error Control: The data link layer imposes error control mechanism to identify lost or damaged frames, duplicateframes and then retransmit them.
• Access Control: The data link layer imposes access control mechanism to determine which device has right to send data in an multipoint connection setting.
• Main Responsibility: The main responsibility of the data link layer is hop to hop transmission of frames.

Data Communication and Computer Networking module | PDF page 16 | lines 2-17

• At the sending side, the transport layer receives data from the session layer, divides it into units called segments and sends it to the network layer.
• To ensure process to process delivery the transport layer makes use of port address to identify the data from the sending and receiving process.

• The data can be transported in a connection oriented or connectionless manner.
• The Transport layer is responsible for segmentation and reassembly of the message into segments which bear sequence numbers.
• The transport layer also carries out flow control and error control functions; but unlike data link layer these are end to end rather than node to node.
• The main responsibility of the transport layer is process to process delivery of the entire message

Data Communication and Computer Networking module | PDF page 14 | lines 12-29

The Open Systems Interconnection (OSI) Model was developed by International Organization for Standardization (ISO). ISO is the organization, OSI is the model
It was developed to allow systems with different platforms (Hardware & software) to communicate with each other.
Now, it is a network model that defines the protocols for network communications.
It is a hierarchical model that groups its processes into seven (7) layers. (Top to Bottom)
1. Application Layer
2. Presentation Layer
3. Session Layer
4. Transport Layer
5. Network Layer
6. Data Link Layer
7. Physical Layer
Each layer has specific functions to perform and has to co-operate with the layers above and below it.

Question sources

Computer Science model exam 2 · Question 50

Question 73 | Q00710

What is the technique of combining multiple input signals or streams onto a shared transmission link?

A. Broadcast

B. Multicast

C. Multiplexing

D. demultiplexing

Hint

Compare the signal mechanism, medium properties or transmission direction against the definitions and stated physical assumptions.

Answer C: Multiplexing

Multiplexing combines input signals or streams so they share a link, using distinctions such as frequency, wavelength or time slots. Demultiplexing is the corresponding receiver operation that separates them. Broadcast and multicast instead describe recipient sets for a message. Link sharing and destination distribution therefore answer different questions, even though a network can use both mechanisms.

Why each choice is right or wrong

A - Incorrect: Broadcast distributes a message to all members of a broadcast domain rather than combining input streams.

B - Incorrect: Multicast distributes to a receiver group rather than combining inputs onto a link.

C - Correct: Multiplexing combines inputs onto the shared link.

D - Incorrect: Demultiplexing separates received multiplexed inputs; it is the reverse operation.

Primary note proof

Study-note section NET32

> Multiplexing combines multiple input streams onto a shared link; demultiplexing separates them at the receiver. It differs from broadcasting one message to many destinations. FDM assigns distinct frequency bands with suitable guard spacing; WDM assigns different optical wavelengths. TDM allocates time slots: synchronous TDM reserves recurrent slots even if an input is idle, while statistical TDM allocates according to demand and needs identification.

Study-note section NET30

> Flooding sends copies on eligible outgoing links with duplicate/lifetime controls; random walk picks a neighbor probabilistically. Unicast targets one destination, broadcast all in a scope, multicast a subscribed group and anycast one member sharing an address, normally nearest under routing metrics. Multi-destination packets can list multiple targets; this is not necessarily identical to broadcast. Group multicast trees use mechanisms such as reverse-path checks; Ethernet spanning tree is a different layer-2 mechanism.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 20 | lines 37-42

> MULTIPLEXING
> Whenever the bandwidth of a medium linking two devices is greater than the bandwidth needs of the devices, the link can be shared. Multiplexing is the set of techniques that allows the simultaneous transmission of multiple signals across a single data link.

Data Communication and Computer Networking module | PDF page 17 | lines 54-59

> ICMP- Internet Control Message Protocol: It is a signaling mechanism used to inform the sender about datagram problemsthat occur during transit. It is used by intermediate devices.
> IGMP- Internet Group Message Protocol: It is a mechanism that allows sending the same message to a group of recipients.

Question sources

Computer Science model exam 2 · Question 51

Question 74 | Q00912

How many layers are there in OSI reference model?

A. 7

B. 6

C. 5

D. 4

Hint

Match the requested scope or data unit to the layer duties in the note; distinguish hop delivery from end-to-end process delivery.

Answer A: 7

OSI is explicitly a seven-layer hierarchy. Evidence: PDF 14, 17.

Why each choice is right or wrong

A - Correct: Seven is the stated count (PDF 14, 17.)

B - Incorrect: Six omits one stated layer (PDF 14, 17.)

C - Incorrect: Five is not the stated OSI count (PDF 14, 17.)

D - Incorrect: Four is the original TCP/IP count (PDF 14, 17.)

Primary note proof

Study-note section NET03

> A reference model divides responsibilities and interfaces; it is not itself executable networking software. OSI is a seven-layer reference model; TCP/IP describes an implemented protocol suite, usually taught with four layers. A five-layer teaching model separates physical and link functions. State the model before counting layers.

Study-note section NET19

> The four-layer TCP/IP model folds OSI layers 5-7 into application, retains transport, calls layer 3 Internet, and combines link/physical as network access. A model is a guide to functions, not a

guarantee that every application gets a reliable network. Distinguish end-to-end application service from its underlying process-to-process transport.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 14 | lines 12-29

The Open Systems Interconnection (OSI) Model was
developed by International Organization for Standardization
(ISO). ISO is the organization, OSI is the model
It was developed to allow systems with different platforms
(Hardware & software) to communicate with each other.
Now, it is a network model that defines the protocols for
network communications.
It is a hierarchical model that groups its processes into seven
(7) layers. (Top to Bottom)
1. Application Layer
2. Presentation Layer
3. Session Layer
4. Transport Layer
5. Network Layer
6. Data Link Layer
7. Physical Layer
Each layer has specific functions to perform and has to co-
operate with the layers above and below it.

Data Communication and Computer Networking module | PDF page 17 | lines 3-15

The structure TCP/IP model is very similar to the
structure of the OSI reference model. The OSI model has
seven layers where the TCP/IP model has four layers.
• The Application layer of TCP/IP model
corresponds to the Application Layer of Session,
Presentation & Application Layer of OSI model.
• The Transport layer of TCP/IP model corresponds
to theTransport Layer of OSI model
• The Network layer of TCP/IP model corresponds
to the Network Layer of OSI model
• The Host to network layer of TCP/IP model
correspondsto the Physical and Data link Layer of
OSI model.

Question sources

Computer Science Exit Exam · 2018 · Question 25

Question 75 | Q00921

Which one of the following ip address class uses first two octets for network addresses and last two for host addressing?

A. Class C

B. Class D

C. Class A

D. Class B

Hint

Convert the mask to a prefix, separate network and host bits, and apply the relevant subnet-count or usable-host rule.

Answer D: Class B

Two octets are sixteen bits. A historical Class B default /16 therefore uses the first two octets as network bits and the final two as host bits. Class A defaults to one network octet and Class C to three; Class D is multicast. Actual CIDR allocation can override the historical defaults.

Why each choice is right or wrong

A - Incorrect: Class C defaults to /24, using three network octets and one host octet.

B - Incorrect: Class D denotes multicast and does not use the described ordinary network/host division.

C - Incorrect: Class A defaults to /8, using one network octet and three host octets.

D - Correct: Class B defaults to /16, exactly the two-network-octet, two-host-octet division described.

Primary note proof

Study-note section NET22

> Historical classes use leading patterns: A 0 with /8, B 10 with /16, C 110 with /24; D 1110 is multicast and E 1111 reserved. Ordinary class-A first octets are 1-126 because 0 and 127 have special uses. B spans 128-191 and C 192-223. Default usable counts are 2^24-2, 2^16-2 and 254. Modern CIDR requires the actual prefix and overrides class defaults.

Study-note section NET24

> A /p IPv4 prefix has p leading one bits followed by 32-p zeros. Partial octet masks are 128,192,224,240,248,252,254. /19 is 255.255.224.0; /20 is 255.255.240.0; /21 is 255.255.248.0, correcting the study guide’s 255.248.0.0 mistake.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 19 | lines 23-36

Classful addressing : In classful addressing, the addressspace is divided into five classes: A, B, C, D, and E.
• Netid and Hostid In classful addressing, an IP addressin class A, B, or C is divided into netid and hostid.
Subnetting: It allows a network to be split into several parts for internal use but still act like a single network to the outsideworld.
• To implement subnetting, the router needs a subnet mask that indicates the split between network + subnet number and host. Ex. 255.255.252.0/22. A‖/22‖ to indicate that the subnet mask is 22 bits long.

Question sources

Computer Science Exit Exam · 2018 · Question 34

Question 76 | Q00950

Which of the following OSI layers is NOT correctly matched to its corresponding data

Units (PDU)?

A. Application layer ---> Data

B. Transport layer ---> Segment

C. ¢.

Physical layer ---> Bit

D. Network layer ---> Frame

Hint

Match the requested scope or data unit to the layer duties in the note; distinguish hop delivery from end-to-end process delivery.

Answer D: Network layer ---> Frame

Network data units are packets, while frames are data-link units. The other options follow the described bit/segment and upper-data roles. Evidence: PDF 16, 15, 15, 14, 16.

Why each choice is right or wrong

A - Incorrect: Application handles user data

B - Incorrect: Transport explicitly forms segments

C - Incorrect: Physical transmits bits

D - Correct: Frame belongs to data link; network is packet

Primary note proof

Study-note section NET12

Sending proceeds from application data to transport segment/datagram, network packet, link frame and physical bits/symbols; receiving reverses the order. Each layer serves the layer above. A router removes a received link frame, inspects IP, and creates a new link frame for the next hop. MAC addresses usually change across routed hops; end-to-end IP addresses ordinarily remain until translation.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 16 | lines 2-17

• At the sending side, the transport layer receives data from the session layer, divides it into units called segments and sends it to the network layer.
• To ensure process to process delivery the transport layer makes use of port address to identify the data from the sending and receiving process.
• The data can be transported in a connection oriented or connectionless manner.
• The Transport layer is responsible for segmentation and reassembly of the message into segments which bear sequence numbers.
• The transport layer also carries out flow control and error control functions; but unlike data link layer these are end to end rather than node to node.
• The main responsibility of the transport layer is process to process delivery of the entire message

Data Communication and Computer Networking module | PDF page 15 | lines 41-61

Network Layer
• The network layer makes sure that the data is deliveredto the receiver despite multiple intermediate devices.
• The network layer at the sending side accepts data from the transport layer, divides it into packets, addsaddressing information in the header and passes it tothe data link layer.
• The network layer is responsible for source todestination of delivery of data.
• The network layer uses logical address commonlyknown as IP address to recognize devices on the network.
• Each packet is independent of the other and may travelusing different routes to reach the receiver hence may arrive out of turn at the receiver

(Routing).
• The Network layer does not perform any flow controlor error control
• The main responsibility of Network Layer is transmission of packets from source to destination

Data Communication and Computer Networking module | PDF page 15 | lines 13-40

Data Link Layer
• The Data Link layer adds reliability to the physical layer by providing error detection and correction mechanisms.
• Framing: the Data Link layer receives the data from Network Layer and divides the stream of bits into fixed size manageable units called as Frames and sends it to the physical layer. On the receiver side, the data link layer receives the stream of bits from the physical layer and regroups them into frames and sends them to the Network layer.
• Physical Addressing: The Data link layer appends the physical address in the header of the frame before sending it to physical layer.
• Flow control: The data link layer makes sure that the sender sends the data at a speed at which the receiver canreceive it else if there is an overflow at the receiver sidethe data will be lost.
• Error Control: The data link layer imposes error control mechanism to identify lost or damaged frames, duplicateframes and then retransmit them.
• Access Control: The data link layer imposes access control mechanism to determine which device has right to send data in an multipoint connection setting.
• Main Responsibility: The main responsibility of the data link layer is hop to hop transmission of frames.

Data Communication and Computer Networking module | PDF page 14 | lines 32-49

Physical Layer:
• The Physical Layer provides a standardized interface to physical transmission media, including: Mechanical specification of electrical connectors and cables, for example maximum cable length, Electrical specification of transmission line and Bit-by-bit or symbol-by-symbol delivery.
• Interface: The Physical Layer defines the characteristics of interfaces between the devices & transmission medium.

• Representation of bits: The physical layer is concerned with transmission of signals from one device to another which involves converting data (1_s & 0_s) into signals and vice versa. It is not concerned with the meaning or interpretation of bits.
• Data rate: The physical layer defines the data transmission rate i.e. number of bits sent per second. It is the responsibility of the physical layer to maintain the defined data rate.

Data Communication and Computer Networking module | PDF page 16 | lines 43-47

Application Layer
• The application layer enables the user to communicate its data to the receiver by providing certain services.
• The main Responsibility of Application layer is to provide the user access to network resources.

Question sources

Computer Science Exit Exam · 2018 · Question 63

Question 77 | Q00959

Which of the following layers is responsible for encryption, translation and compression?

A. Presentation layer

B. Data link layer

C. .
Transport layer

D. Network layer

Hint

Match the requested scope or data unit to the layer duties in the note; distinguish hop delivery from end-to-end process delivery.

Answer A: Presentation layer

The presentation paragraph explicitly names translation, encryption and compression together. Evidence: PDF 16, 15, 16, 15.

Why each choice is right or wrong

A - Correct: All three functions appear in the presentation definition (PDF 16, 15, 16, 15.)

B - Incorrect: Data link handles frames and link control (PDF 16, 15, 16, 15.)

C - Incorrect: Transport handles segmentation and process delivery (PDF 16, 15, 16, 15.)

D - Incorrect: Network handles addressing and routes (PDF 16, 15, 16, 15.)

Primary note proof

Study-note section NET19

OSI session roles establish/manage dialogs and can coordinate checkpoints so transfer resumes after interruption. Presentation roles translate encodings and handle compression/encryption. Compression reduces representation size; encryption hides content and need not shrink it. Application protocols provide services directly to applications. Practical implementations distribute these functions differently; TLS is not proof of a separate physical presentation-layer device.

Study-note section NET12

Sending proceeds from application data to transport segment/datagram, network packet, link frame and physical bits/symbols; receiving reverses the order. Each layer serves the layer above. A router removes a received link frame, inspects IP, and creates a new link frame for the next hop. MAC addresses usually change across routed hops; end-to-end IP addresses ordinarily remain until translation.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 16 | lines 33-42

Presentation Layer
• The communicating devices may be having different platforms. The presentation layer performs translation, encryption and compression of data.
• The presentation layer receives the data from the application layer adds header which contains information related to encryption and compression and sends it to the session layer.
• So, the main responsibility of the Presentation layer is translation, compression and encryption.

Data Communication and Computer Networking module | PDF page 15 | lines 13-40

Data Link Layer
• The Data Link layer adds reliability to the physical layer by providing error detection and correction mechanisms.
• Framing: the Data Link layer receives the data from Network Layer and divides the stream of bits into fixed size manageable units called as Frames and sends it to the physical layer. On the receiver side, the data link layer receives the stream of bits from the physical layer and regroups them into frames and sends them to the Network layer.
• Physical Addressing: The Data link layer appends the physical address in the header of the frame before sending it to physical layer.

• Flow control: The data link layer makes sure that the sender sends the data at a speed at which the receiver canreceive it else if there is an overflow at the receiver sidethe data will be lost.
• Error Control: The data link layer imposes error control mechanism to identify lost or damaged frames, duplicateframes and then retransmit them.
• Access Control: The data link layer imposes access control mechanism to determine which device has right to send data in an multipoint connection setting.
• Main Responsibility: The main responsibility of the data link layer is hop to hop transmission of frames.

Data Communication and Computer Networking module | PDF page 16 | lines 2-17

• At the sending side, the transport layer receives data from the session layer, divides it into units called segments and sends it to the network layer.
• To ensure process to process delivery the transport layer makes use of port address to identify the data from the sending and receiving process.
• The data can be transported in a connection oriented or connectionless manner.
• The Transport layer is responsible for segmentation and reassembly of the message into segments which bear sequence numbers.
• The transport layer also carries out flow control and error control functions; but unlike data link layer these are end to end rather than node to node.
• The main responsibility of the transport layer is process to process delivery of the entire message

Data Communication and Computer Networking module | PDF page 15 | lines 41-61

Network Layer
• The network layer makes sure that the data is deliveredto the receiver despite multiple intermediate devices.
• The network layer at the sending side accepts data from the transport layer, divides it into packets, addsaddressing information in the header and passes it tothe data link layer.
• The network layer is responsible for source todestination of delivery of data.
• The network layer uses logical address commonlyknown as IP address to recognize

devices on the network.
• Each packet is independent of the other and may travelusing different routes to reach the receiver hence may arrive out of turn at the receiver (Routing).
• The Network layer does not perform any flow controlor error control
• The main responsibility of Network Layer is transmission of packets from source to destination

Question sources

Computer Science Exit Exam · 2018 · Question 72

Question 78 | Q00962

Which service used to translate domain names to ip address?

A. HTTPS

B. DHCP

C. HTTP

D. DNS

Hint

Separate address width, syntax, reserved scope and the supplied prefix or historical classful convention.

Answer D: DNS

DNS is explicitly the external naming service and Domain Name Service; the hosts-file passage contrasts it with stored host addresses. Evidence: PDF 18, 65, 28.

Why each choice is right or wrong

A - Incorrect: HTTPS is listed by port, not as naming service (PDF 18, 65, 28.)

B - Incorrect: DHCP is host configuration, not the named DNS service (PDF 18, 65, 28.)

C - Incorrect: HTTP is not named as the naming service (PDF 18, 65, 28.)

D - Correct: DNS matches the domain naming function (PDF 18, 65, 28.)

Primary note proof

Study-note section NET20

DNS resolves names to records, including IPv4 A and IPv6 AAAA addresses; it can use UDP or TCP port 53. DHCP dynamically leases IPv4 settings, commonly address, mask, gateway and DNS server. Its basic exchange is discover, offer, request, acknowledge. IP itself does not assign addresses.

Study-note section NET21

HTTP defines web request/response semantics; it is stateless, and a message body may be absent. HTTPS adds TLS protection. FTP transfers files using control and separate data connections; it is not the same protocol as SFTP. SMTP submits and relays mail; POP3 retrieves messages and IMAP accesses/synchronizes server mailboxes. Saying SMTP handles both sending and end-user mailbox retrieval is inaccurate.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 18 | lines 27-32

Application Layer
The Application Layer is a combination of Session,
Presentation & Application Layers of OSI models and defines
high level protocols like File Transfer (FTP), Electronic Mail
(SMTP), Virtual Terminal (TELNET), Domain Name Service
(DNS), etc.

Data Communication and Computer Networking module | PDF page 65 | lines 31-38

/etc/hosts
The /etc/hosts file always contains the localhost IP
address, 127.0.0.1, which is
usedfor interprocess communication.
Never remove this line! Sometimes contains
addresses of additional hosts, whichcan be contacted
without using an external naming service such as
DNS (the Domain Name Server).

Data Communication and Computer Networking module | PDF page 28 | lines 32-45

Application Layer
The application layer in TCP/IP is equivalent to the
combined session, presentation, and application layers in
the OSI model and many protocols are defined at this
layer.
The Process/Application Layer Protocols
• Telnet
• File Transfer Protocol (FTP)
• Network File System (NFS).
• Simple Mail Transfer Protocol (SMTP
• POP3 is used to receive mail.
• Simple Network Management Protocol (SNMP)
• Domain Name Service (DNS)
• Dynamic Host Configuration Protocol (DHCP)

Question sources

Computer Science Exit Exam · 2018 · Question 75

Question 79 | Q00968

Which scenario is best suited for UDP rather than TCP protocol?

A. Live video streaming

B. Email transmission

C. Downloading the files

D. Database update

Hint

Identify the requested service or delivery guarantee, then distinguish application roles, transport behavior and address configuration.

Answer A: Live video streaming

UDP is connectionless and omits flow/error control, fitting live streams where timely delivery matters more than repairing old data. Email/file/database transactions need the reliability contrast rather than that latency preference. Evidence: PDF 18, 18.

Why each choice is right or wrong

A - Correct: Live streaming fits the no-repair-delay tradeoff (PDF 18, 18.)

B - Incorrect: Mail transfer is an application for which reliable delivery is preferable (PDF 18, 18.)

C - Incorrect: File download generally needs intact reliable bytes (PDF 18, 18.)

D - Incorrect: Database updates require dependable ordered delivery (PDF 18, 18.)

Primary note proof

Study-note section NET17

> TCP offers a reliable ordered byte stream using sequence numbers, acknowledgments, retransmission and windows. Flow control protects the receiver; congestion control protects network capacity. UDP sends independent datagrams with ports and a checksum but no built-in setup, delivery guarantee, retransmission or ordering. Live interactive traffic may choose UDP when late data is less useful than lost data. Application protocols can add reliability over UDP.

Study-note section NET21

> HTTP defines web request/response semantics; it is stateless, and a message body may be absent. HTTPS adds TLS protection. FTP transfers files using control and separate data connections; it is not the same protocol as SFTP. SMTP submits and relays mail; POP3 retrieves messages and IMAP accesses/synchronizes server mailboxes. Saying SMTP handles both sending and end-user mailbox retrieval is inaccurate.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 18 | lines 9-21

TCP - Transmission Control Protocol: TCP is a reliable connection-oriented, reliable protocol. i.e. a connection is established between the sender and receiver before the data can be transmitted. It divides the data it receives from the upper layer into segments and tags a sequence number to each segment which is used at the receiving end for reordering of data.
UDP - User Datagram Protocol: UDP is a simple protocol used for process to process transmission. It is an unreliable, connectionless protocol for applications that do not require flow control or error control. It simply adds port address, checksum and length information to the data it receives from the upper layer.

Data Communication and Computer Networking module | PDF page 18 | lines 27-32

Application Layer
The Application Layer is a combination of Session, Presentation & Application Layers of OSI models and defines high level protocols like File Transfer (FTP), Electronic Mail (SMTP), Virtual Terminal (TELNET), Domain Name Service (DNS), etc.

Question sources

Computer Science Exit Exam · 2018 · Question 81

Question 80 | Q00976

Assume that you have IPv4 addresses in binary notation 11000001 10000011 00011011 11111111 and you are requested to change into dotted decimal notation. What is the equivalent IP address in decimal dotted notation?

A. 192.174.27.255

B. 192.134.67.254

C. ¢.
193.130.28.254

D. 193.131.27.255

Hint

Sum the eight bit weights in each octet independently, then preserve their order in dotted-decimal notation.

Answer D: 193.131.27.255

Compute each octet: 11000001=128+64+1=193; 10000011=128+2+1=131; 00011011=16+8+2+1=27; 11111111=255. Evidence: PDF 19.

Why each choice is right or wrong

A - Incorrect: First and second octets disagree with 193 and 131 (PDF 19.)

B - Incorrect: 192,134,67,254 disagree with the independently converted octets 193,131,27,255 (PDF19).

C - Incorrect: Only first octet matches; 130,28,254 do not (PDF 19.)

D - Correct: 193.131.27.255 matches all four converted octets (PDF 19.)

Primary note proof

Study-note section NET22

> Write IPv4 as four decimal octets 0-255, or as 32 binary bits. Use weights 128,64,32,16,8,4,2,1 within each octet. Thus 11000001 10000011 00011011 11111111 is 193.131.27.255. A value such as 257 is impossible. Syntactic validity differs from assignability: an address ending .0 or .255 can be a host under some prefixes.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 19 | lines 2-22

> Address Space: An address space is the total
> number ofaddresses used by the protocol.
> • If a protocol uses N bits to define an address,
> the address space is 2N
> because each bit can
> have twodifferent values (0 or 1) and N bits
> can have 2N values.
> • IPv4 uses 32-bit addresses, which means that
> the address space is 232 or 4,294,967,296
> (more than 4billion).
> Notations: There are two notations to show an IPv4 address:
> • Binary notation: The IPv4 address is displayed
> as 32bits. ex. 11000001 10000011 00011011
> 11111111
> • Dotted decimal notation: To make the IPv4
> address easier to read, Internet addresses are
> usually written in decimal form with a decimal
> point (dot) separatingthe bytes. Each byte (octet)
> is 8 bits hence each number in dotted-decimal
> notation is a value rangingfrom 0 to 255. Ex.
> 129.11.11.239

Question sources

Computer Science Exit Exam · 2018 · Question 89

Question 81 | Q00979

Which one of the following is disadvantage of circuit switching?

A. Predictable performance

B. Low latency

C. Guaranteed bandwidth

D. Limited scalability

Hint

Compare signal repetition, frame forwarding, packet routing and policy enforcement using the stated device or traffic assumptions.

Answer D: Limited scalability due to reserved resources

Circuit switching reserves resources for an established path. NET31 explains that this offers predictable bandwidth but introduces setup, blocking and unused reservation during silence. Those costs constrain how many simultaneous circuits can be supported as demand grows, making limited scalability the disadvantage among the offered choices.

Why each choice is right or wrong

A - Incorrect: Predictable performance is a benefit of allocated circuit resources, not the disadvantage requested.

B - Incorrect: Low transfer latency after setup can be beneficial; the relevant costs include setup and resource reservation.

C - Incorrect: Guaranteed allocated bandwidth is an advantage, although reserving it consumes capacity during silence.

D - Correct: Finite reserved resources and blocking constrain simultaneous connections and therefore scalability as demand grows.

Primary note proof

Study-note section NET31

> Circuit switching sets up a path with reserved resources, transfers data, then releases it. Predictable allocated bandwidth trades against setup/blocking and wasted reservation during silence. A traditional telephone call is the standard example. Packet switching divides data into packets that share links statistically; queueing can add variable delay and loss. This does not make modern voice-over-packet impossible: buffering, scheduling and capacity planning manage it.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 20 | lines 12-26

> Circuit Switching: In circuit switching, two
> communicating stations are connected by a dedicated

communication path which consists of intermediate nodes in the network and the links that connect these nodes.
It involved the following three distinct steps
• Circuit Establishment: To establish an end-to-end connection before any transfer of data.
• Data transfer: Transfer data is from the source to the destination. The data may be analog or digital, depending on the nature of the network. The connection is generally full-duplex.
• Circuit disconnect: Terminate connection at the end of data transfer. Signals must be propagated to deallocate the dedicated resources.

Data Communication and Computer Networking module | PDF page 20 | lines 27-36

Message Switching:
Packet Switching: Packet switching was designed to address the shortcomings of circuit switching in dealing with data communication. Unlike circuit switching where communication is continuous along a dedicated circuit, in packet switching, communication is discrete in form of packets.
The three switching modes to choose from are:
• Cut-through
• Store-and-forward
• Fragment-free

Question sources

Computer Science Exit Exam · 2018 · Question 92

Question 82 | Q00997

In which case must a dedicated communication path between the sender and receiver be established?

A. Circuit switching

B. Packet switching

C. A and B

D. None of the above

Hint

Use the cited note definitions to identify the requested function or scope, then check each alternative against that same rule.

Answer A: Circuit switching

A dedicated path is explicitly required by circuit switching. Packet communication is contrasted with that continuous dedicated circuit.

Why each choice is right or wrong

A - Correct: Circuit establishment creates the dedicated path

B - Incorrect: Packet communication is discrete rather than the dedicated circuit

C - Incorrect: Both incorrectly adds a requirement not inherent to packet switching

D - Incorrect: None excludes the explicitly dedicated circuit

Primary note proof

Study-note section NET31

> Circuit switching sets up a path with reserved resources, transfers data, then releases it. Predictable allocated bandwidth trades against setup/blocking and wasted reservation during silence. A traditional telephone call is the standard example. Packet switching divides data into packets that share links statistically; queueing can add variable delay and loss. This does not make modern voice-over-packet impossible: buffering, scheduling and capacity planning manage it.

Study-note section NET31

> Datagram packets are forwarded independently. Virtual circuits establish forwarding state, but resource reservation is optional, not a necessary property of every virtual circuit. Message switching stores a complete message before forwarding, without a dedicated end-to-end path. Packet store-and-forward waits for the full packet/frame; cut-through starts after enough header arrives; fragment-free historically waits through the initial collision-sensitive portion. No routing algorithm guarantees that every packet always takes the geometrically shortest route.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 20 | lines 12-26

> Circuit Switching: In circuit switching, two
> communicating stations are connected by a dedicated
> communication path which consists of intermediate
> nodes in the network and the links that connect these
> nodes.
> It involved the following three distinct steps
> • Circuit Establishment: To establish an end-to-end
> connection before any transfer of data.
> • Data transfer: Transfer data is from the source to the
> destination. The data may be analog or digital,
> depending on the nature of the network. The
> connection is generally full-duplex.
> • Circuit disconnect: Terminate connection at the end

of data transfer. Signals must be propagated to deallocate the dedicated resources.

Data Communication and Computer Networking module | PDF page 20 | lines 27-36

Message Switching:
Packet Switching: Packet switching was designed to address the shortcomings of circuit switching in dealing with data communication. Unlike circuit switching where communication is continuous along a dedicated circuit, in packet switching, communication is discrete in form of packets.
The three switching modes to choose from are:
• Cut-through
• Store-and-forward
• Fragment-free

Question sources

National Exit Exam practice questions · Question 11

Computer Science Exit Exam practice collection · Question 151

Question 83 | Q00999

Which one of the following is a type of network topology in which all devices in the network are interconnected?

A. Star Topology

B. Ring Topology

C. Mesh Topology

D. Tree Topology

Hint

Draw the links and identify shared components, alternate paths and the effect of the specified failure or growth requirement.

Answer C: Mesh Topology

Interpret interconnected as every node directly connected to every other node: this is the module full-mesh definition. Without directly, all connected topologies would qualify. Evidence: PDF 23, 23, 23.

Why each choice is right or wrong

A - Incorrect: Star nodes connect through a central device (PDF 23, 23, 23.)

B - Incorrect: Ring nodes directly connect only to two neighbors (PDF 23, 23, 23.)

C - Correct: Full mesh explicitly connects every node to every other (PDF 23, 23, 23.)

D - Incorrect: Tree is listed but not defined as all-pairs direct connectivity (PDF 23, 23, 23.)

Primary note proof

Study-note section NET08

Physical topology describes link layout; logical topology describes communication/access relationships. Point-to-point links join two endpoints; multipoint links share a medium. A full mesh consists of point-to-point links.

Study-note section NET08

Bus uses a shared backbone; an unterminated break can disrupt the segment. Star connects endpoints through a central device: one edge failure isolates that endpoint, whereas central failure affects the star. Ring forms a loop; basic single rings are vulnerable to a break, while protected dual rings differ. Token passing is associated with Token Ring but is an access method, not a necessary property of every ring. Tree is hierarchical; hybrid combines arrangements.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 23 | lines 45-53

Mesh Topology: in this topology devices are connected with many redundant interconnections between network nodes. In a full mesh topology, every node has a connection to every other node in the network, which makes it the most expensive topology over all the other topologies. The number of cables grows fast as the number of nodes increases, and it can be calculated by using the general formula ((n (n - 1)) /2), where n is the number of nodes in the

Data Communication and Computer Networking module | PDF page 23 | lines 19-34

Star Topology: in this topology, each node is connected directly to a central device called a hub or a switch. Data on a star network passes through the central device (switch) before continuing to its destination. The central device manages and controls all functions of the network. This configuration is common with twisted pair cable. RJ-45 Connectors are used to connect the cable to the Network Interface Card (NIC) of each computer. Its advantages include, ease of installation and reconfiguration, robust (ease of fault identification and isolation), link failure only affects device(s) connected to that link, and is less expensive than mesh. Its drawbacks include more cable requirements (than bus and ring) and single point of failure (if central device fail, the whole system will be down).

Data Communication and Computer Networking module | PDF page 23 | lines 35-44

Ring Topology: in this topology, all devices are connected to one another in the shape of a closed loop, so that each device is connected directly to two other devices, one on either side of it. Some of its advantages include, easy to install and reconfigure, less expensive (than mesh), and performance is even despite the number of users. Its cons include, break in the ring (such as a disabled station) can disable the entire network, and limitations on media and traffic (limitation on ring length and number of devices).

Question sources

National Exit Exam practice questions · Question 13

Computer Science Exit Exam practice collection · Question 152

Question 84 | Q01004

Which statements about IPv4 and IPv6 addresses are correct? Select all that apply.

A. IPv4 is 128-bit and IPv6 is 28-bit

B. IPv4 is physical address

C. IPv6 is logical address

D. IPv4 is 32-bit and IPv6 is 128-bit

Hint

Separate address width, syntax, reserved scope and the supplied prefix or historical classful convention.

Answer C, D: IPv6 is logical address; IPv4 is 32-bit and IPv6 is 128-bit

IPv4 addresses contain 32 bits, and IPv6 addresses contain 128 bits. Both are logical network-layer addresses, so IPv6 being logical is compatible with the width comparison. Physical or MAC addressing belongs to the link layer. The corrected selection instruction allows both true statements to be selected while retaining the original factual comparisons and the two incorrect distractors.

Why each choice is right or wrong

A - Incorrect: IPv4 is 32 bits and IPv6 is 128 bits; neither printed width is correct.

B - Incorrect: IPv4 is network-layer logical addressing, not a physical/MAC address.

C - Correct: IPv6 addresses identify network-layer endpoints logically rather than physical link interfaces.

D - Correct: This gives the correct address lengths: 32 bits for IPv4 and 128 for IPv6.

Primary note proof

Study-note section NET16

IP supplies connectionless best-effort packet delivery, not end-to-end ordering or retransmission. IPv4 addresses are 32 bits. Its minimum header is 20 bytes and can grow to 60 bytes; it is not a 32-bit header. IHL counts 32-bit words; total length includes header and payload. TTL limits lifetime across routers; the protocol field identifies TCP, UDP or another upper-layer protocol.

Study-note section NET23

IPv6 has 128-bit hexadecimal addresses, flexible prefixes and no IPv4-style broadcast. Sources, not routers, fragment IPv6 packets. IPv6 does not automatically encrypt traffic or make authentication unnecessary. Compare IPv6's larger 128-bit address space and encryption support separately; specify the property being evaluated.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 18 | lines 45-54

IP addresses: IP address uniquely identifies a device on the
Internet. Every host and router on the Internet has an IP address,
which encodes its network number and host number.
• The combination is unique: in principle, no two
machines on the Internet have the same IP address.
• An IPv4 address is 32 bits long
• They are used in the Source address and Destination
address fields of IP packets.
• An IP address does not refer to a host but it refers to a
network interface.

Data Communication and Computer Networking module | PDF page 19 | lines 45-49

NAT (Network Address Translation): The scarcity of
network addresses in IPv4 led to the development of IPv6.
Due to this, we need to use private IP address inside the
organization and translate it to public IP address using
NAT.

Question sources

National Exit Exam practice questions · Question 18

Computer Science Exit Exam practice collection · Question 154

Question 85 | Q01006

Which one of the data communication mediums is used for direct transmission?

A. Induced

B. Crosstalk

C. A and B

D. None of the above

Hint

Compare the signal mechanism, medium properties or transmission direction against the definitions and stated physical assumptions.

Answer D: Neither induced nor crosstalk names a transmission medium

The note identifies cables and unguided radio/microwave/infrared as transmission media. Crosstalk instead names interference from nearby channels in NET06, and induced alone does not name a medium in the note. Regardless of the vague direct-transmission phrase, none of A-C supplies a listed medium, so D is the supported exclusion response.

Why each choice is right or wrong

A - Incorrect: Induced is not a transmission-medium category established here.

B - Incorrect: Crosstalk is unwanted coupling/interference, not a medium for intentional direct transmission.

C - Incorrect: Combining two nonmedium terms does not supply the requested transmission medium.

D - Correct: Neither induced nor crosstalk names a transmission medium among the choices.

Primary note proof

Study-note section NET07

> Radio, microwave and infrared are unguided media. Ground waves follow Earth, sky waves can reflect from ionized layers, and line-of-sight paths require suitable visibility. Microwaves are radio waves in the broader physical classification. Infrared generally does not penetrate walls. Directionality depends on antennas: omnidirectional means broad azimuth coverage, not equal radiation in every 3-D direction. Legacy Ethernet straight-through cables join unlike MDI/MDI-X roles; crossover joins like roles, such as PC-PC or switch-switch. Auto-MDI-X can remove that requirement.

Study-note section NET06

> Attenuation reduces signal strength. Distortion changes shape, often because frequencies have different delays. Noise adds unwanted energy: thermal noise comes from random thermal motion, crosstalk leaks from nearby channels, and impulse noise is a short disturbance. Amplifiers amplify noise too; digital repeaters regenerate decisions but cannot reconstruct every corrupted bit.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 10 | lines 36-55

TRANSMISSION MEDIA
Transmission media is a means by which a communicationsignal is carried from one system to another
A transmission medium can be defined as anything that cancarry information from a source to a destination. The transmission medium is usually free space, metallic cable orfiber optic cable. Guided and Unguided (WIRELESS) Guided Transmission Media uses a cabling system that guidesthe data signals along a specific path. Out of these twisted-paircable, coaxial cable transport signals in the form of electricsignals and fiber-optic cable transport signals in the form oflight.
Unguided Transmission Media transport data without using a physical conductor. It uses wireless electromagnetic signals to send data. Three types of unguided media:
• Radio waves
• Micro waves
• Infrared.

Data Communication and Computer Networking module | PDF page 10 | lines 18-35

receiver.There are three causes of impairment:
• Attenuation
• Distortion
• Noise
Attenuation
Attenuation results in loss of energy due to distance. Whena signal travels through a medium, it loses some of its energy in overcoming the resistance of the medium. The electrical energy in the signal may convert to heat. To compensate for this loss, amplifiers are used to amplify thesignal.
Distortion
Distortion changes the shape of the signal.
Noise
Noise is any unwanted signal that is mixed or combined with the original signal during transmission. Due to noise the original signal is altered and signal received is not sameas the one sent.

Question sources

National Exit Exam practice questions · Question 20

Computer Science Exit Exam practice collection · Question 153

Question 86 | Q01160

Which OSI layer is responsible for process-to-process delivery and segmentation?

A. Network Layer

B. Transport Layer

C. Physical Layer

D. Data Link Layer

Hint

Match the requested scope or data unit to the layer duties in the note; distinguish hop delivery from end-to-end process delivery.

Answer B: Transport Layer

Transport supplies process-to-process delivery and segmentation. The network layer handles logical addressing and routing, the data-link layer handles hop delivery of frames, and the physical layer transports bits or symbols. Restoring the four readable source rows gives the transport option its proper position. Reliability remains protocol-dependent: identifying transport does not imply that every transport protocol guarantees delivery.

Why each choice is right or wrong

A - Incorrect: Network handles routing and logical addressing rather than process delivery.

B - Correct: Transport supplies process delivery and segmentation.

C - Incorrect: Physical transports signals and bits rather than process messages.

D - Incorrect: Data link supplies hop-local frame delivery rather than process-to-process delivery.

Primary note proof

Study-note section NET17

> TCP offers a reliable ordered byte stream using sequence numbers, acknowledgments, retransmission and windows. Flow control protects the receiver; congestion control protects network capacity. UDP sends independent datagrams with ports and a checksum but no built-in setup, delivery guarantee, retransmission or ordering. Live interactive traffic may choose UDP when late data is less useful than lost data. Application protocols can add reliability over UDP.

Study-note section NET12

> Sending proceeds from application data to transport segment/datagram, network packet, link frame and physical bits/symbols; receiving reverses the order. Each layer serves the layer above. A router removes a received link frame, inspects IP, and creates a new link frame for the next hop. MAC addresses usually change across routed hops; end-to-end IP addresses ordinarily remain until translation.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 16 | lines 2-17

• At the sending side, the transport layer receives data from the session layer, divides it into units called segments and sends it to the network layer.
• To ensure process to process delivery the transport layer makes use of port address to identify the data from the sending and receiving process.
• The data can be transported in a connection oriented or connectionless manner.
• The Transport layer is responsible for segmentation and reassembly of the message into segments which bear sequence numbers.
• The transport layer also carries out flow control and error control functions; but unlike data link layer these are end to end rather than node to node.
• The main responsibility of the transport layer is process to process delivery of the entire message

Data Communication and Computer Networking module | PDF page 15 | lines 41-61

Network Layer
• The network layer makes sure that the data is deliveredto the receiver despite multiple intermediate devices.
• The network layer at the sending side accepts data from the transport layer, divides it into packets, addsaddressing information in the header and passes it tothe data link layer.
• The network layer is responsible for source todestination of delivery of data.
• The network layer uses logical address commonlyknown as IP address to recognize devices on the network.
• Each packet is independent of the other and may travelusing different routes to reach the receiver hence may arrive out of turn at the receiver (Routing).
• The Network layer does not perform any flow controlor error control
• The main responsibility of Network Layer is transmission of packets from source to destination

Data Communication and Computer Networking module | PDF page 14 | lines 32-49

Physical Layer:
• The Physical Layer provides a standardized interface to

physical transmission media, including: Mechanical specification of electrical connectors and cables, for example maximum cable length, Electrical specification of transmission line and Bit-by-bit or symbol-by-symbol delivery.
• Interface: The Physical Layer defines the characteristics of interfaces between the devices & transmission medium.
• Representation of bits: The physical layer is concerned with transmission of signals from one device to another which involves converting data (1_s & 0_s) into signals and vice versa. It is not concerned with the meaning or interpretation of bits.
• Data rate: The physical layer defines the data transmission rate i.e. number of bits sent per second. It is the responsibility of the physical layer to maintain the defined data rate.

Data Communication and Computer Networking module | PDF page 15 | lines 13-40

Data Link Layer
• The Data Link layer adds reliability to the physical layer by providing error detection and correction mechanisms.
• Framing: the Data Link layer receives the data from Network Layer and divides the stream of bits into fixed size manageable units called as Frames and sends it to the physical layer. On the receiver side, the data link layer receives the stream of bits from the physical layer and regroups them into frames and sends them to the Network layer.
• Physical Addressing: The Data link layer appends the physical address in the header of the frame before sending it to physical layer.
• Flow control: The data link layer makes sure that the sender sends the data at a speed at which the receiver canreceive it else if there is an overflow at the receiver sidethe data will be lost.
• Error Control: The data link layer imposes error control mechanism to identify lost or damaged frames, duplicateframes and then retransmit them.
• Access Control: The data link layer imposes access control mechanism to determine which device has right to send data in an multipoint connection setting.
• Main Responsibility: The main responsibility of the data link layer is hop to hop transmission of frames.

Question sources

Computer Science Exit Exam practice questions · Question 21

Question 87 | Q01161

Which IP version uses 32-bit addresses and corresponding 32-bit subnet masks?

A. IPv6

B. IPv4

C. Addressing

D. None of the above

Hint

Convert the mask to a prefix, separate network and host bits, and apply the relevant subnet-count or usable-host rule.

Answer B: IPv4

IPv4 uses 32-bit addresses, commonly written as four decimal octets, and its subnet mask selects a prefix within those 32 bits. IPv6 addresses instead contain 128 bits. The generic word addressing does not identify an IP version, and none of the above fails because the required version is listed.

Why each choice is right or wrong

A - Incorrect: IPv6 uses 128-bit addresses, not the required 32-bit addresses.

B - Correct: IPv4 addresses and their masks contain 32 bits.

C - Incorrect: Addressing is a general activity, not the IP version requested.

D - Incorrect: IPv4 is listed, so none of the above is false.

Primary note proof

Study-note section NET22

> Write IPv4 as four decimal octets 0-255, or as 32 binary bits. Use weights 128,64,32,16,8,4,2,1 within each octet. Thus 11000001 10000011 00011011 11111111 is 193.131.27.255. A value such as 257 is impossible. Syntactic validity differs from assignability: an address ending .0 or .255 can be a host under some prefixes.

Study-note section NET23

> IPv6 has 128-bit hexadecimal addresses, flexible prefixes and no IPv4-style broadcast. Sources, not routers, fragment IPv6 packets. IPv6 does not automatically encrypt traffic or make authentication unnecessary. Compare IPv6's larger 128-bit address space and encryption support separately; specify the property being evaluated.

Study-note section NET24

A /p IPv4 prefix has p leading one bits followed by 32-p zeros. Partial octet masks are 128,192,224,240,248,252,254. /19 is 255.255.224.0; /20 is 255.255.240.0; /21 is 255.255.248.0, correcting the study guide's 255.248.0.0 mistake.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 18 | lines 45-54

IP addresses: IP address uniquely identifies a device on the Internet. Every host and router on the Internet has an IP address, which encodes its network number and host number.
• The combination is unique: in principle, no two machines on the Internet have the same IP address.
• An IPv4 address is 32 bits long
• They are used in the Source address and Destination address fields of IP packets.
• An IP address does not refer to a host but it refers to a network interface.

Data Communication and Computer Networking module | PDF page 19 | lines 23-36

Classful addressing : In classful addressing, the addressspace is divided into five classes: A, B, C, D, and E.
• Netid and Hostid In classful addressing, an IP addressin class A, B, or C is divided into netid and hostid.
Subnetting: It allows a network to be split into several parts for internal use but still act like a single network to the outsideworld.
• To implement subnetting, the router needs a subnet mask that indicates the split between network + subnet number and host. Ex. 255.255.252.0/22. A‖/22‖ to indicate that the subnet mask is 22 bits long.

Question sources

Computer Science Exit Exam practice questions · Question 22

Question 88 | Q01195

What is the main goal of data compression while it paths in different network layers? Its goal is to:

A. Securing data

B. Minimize the size of data

C. Select the best path of destination devices

D. All of the above

Hint

Match the requested scope or data unit to the layer duties in the note; distinguish hop delivery from end-to-end process delivery.

Answer B: Minimize the size of data

NET19 distinguishes reducing representation size from hiding content. Compression targets the amount of data needed to represent information, while encryption provides concealment and routing selects paths. Therefore minimizing size is the compression goal; combining it with security and path selection in the all option misattributes unrelated functions.

Why each choice is right or wrong

A - Incorrect: Securing or concealing content is an encryption/security function, not the primary goal of compression.

B - Correct: Compression reduces representation size, directly matching minimization of data size.

C - Incorrect: Path selection belongs to routing rather than the representation-size transformation performed by compression.

D - Incorrect: Only size reduction describes compression here; security and route selection are separate functions.

Primary note proof

Study-note section NET19

> OSI session roles establish/manage dialogs and can coordinate checkpoints so transfer resumes after interruption. Presentation roles translate encodings and handle compression/encryption. Compression reduces representation size; encryption hides content and need not shrink it. Application protocols provide services directly to applications. Practical implementations distribute these functions differently; TLS is not proof of a separate physical presentation-layer device.

Study-note section NET30

> Routing computes paths; forwarding chooses a next hop for an individual packet. Select the matching route with the longest prefix, then apply the routing system’s tie-breaking criteria. A default /0 matches when nothing more specific does. Static routes are configured; dynamic protocols exchange reachability. Distance vector uses neighbor estimates, while link state

distributes link information and computes shortest paths. Interior protocols operate within an autonomous system; BGP exchanges routes between systems.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 16 | lines 33-42

Presentation Layer
• The communicating devices may be having different platforms. The presentation layer performs translation, encryption and compression of data.
• The presentation layer receives the data from the application layer adds header which contains information related to encryption and compression and sends it to the session layer.
• So, the main responsibility of the Presentation layer is translation, compression and encryption.

Question sources

Computer Science model exam 2 · Question 16

Question 89 | Q01218

Which single option gives the complete set of listed protocols used by end users to retrieve or synchronize stored mailboxes?

A. POP3

B. IMAP

C. SMTP

D. Both POP3 and IMAP

Hint

Identify the requested service or delivery guarantee, then distinguish application roles, transport behavior and address configuration.

Answer D: Both POP3 and IMAP

POP3 retrieves stored messages, while IMAP accesses and synchronizes mailboxes held on the server. SMTP instead submits and relays messages between mail-system components. Since the question asks for the complete set of mailbox-access protocols, either POP3 or IMAP alone is incomplete. The combined choice correctly includes both without assigning mailbox retrieval to the mail transfer protocol.

Why each choice is right or wrong

A - Incorrect: POP3 retrieves messages but alone omits IMAP, so it is an incomplete selection.

B - Incorrect: IMAP accesses mailboxes but alone omits POP3, so it is incomplete.

C - Incorrect: SMTP submits and relays messages; it is not the end-user mailbox retrieval protocol described.

D - Correct: Both POP3 and IMAP provide the requested mailbox-access functions.

Primary note proof

Study-note section NET21

HTTP defines web request/response semantics; it is stateless, and a message body may be absent. HTTPS adds TLS protection. FTP transfers files using control and separate data connections; it is not the same protocol as SFTP. SMTP submits and relays mail; POP3 retrieves messages and IMAP accesses/synchronizes server mailboxes. Saying SMTP handles both sending and end-user mailbox retrieval is inaccurate.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 28 | lines 32-45

Application Layer
The application layer in TCP/IP is equivalent to the
combined session, presentation, and application layers in
the OSI model and many protocols are defined at this
layer.
The Process/Application Layer Protocols
• Telnet
• File Transfer Protocol (FTP)
• Network File System (NFS).
• Simple Mail Transfer Protocol (SMTP
• POP3 is used to receive mail.
• Simple Network Management Protocol (SNMP)
• Domain Name Service (DNS)
• Dynamic Host Configuration Protocol (DHCP)

Data Communication and Computer Networking module | PDF page 18 | lines 27-32

Application Layer
The Application Layer is a combination of Session,
Presentation & Application Layers of OSI models and defines
high level protocols like File Transfer (FTP), Electronic Mail
(SMTP), Virtual Terminal (TELNET), Domain Name Service
(DNS), etc.

Question sources

Computer Science model exam 2 · Question 39

Question 90 | Q01229

The data link layer divides the stream of bits received from the physical layer into manageable data units called _____?

A. Bits

B. Frames

C. Packets

D. Segments

Hint

Match the requested scope or data unit to the layer duties in the note; distinguish hop delivery from end-to-end process delivery.

Answer B: Frames

The receive-side data-link description explicitly regroups physical-layer bits into frames. Evidence: PDF 15, 16, 15, 14.

Why each choice is right or wrong

A - Incorrect: Bits are the incoming physical units, not the regrouped unit (PDF 15, 16, 15, 14.)

B - Correct: Frames are explicitly the regrouped units (PDF 15, 16, 15, 14.)

C - Incorrect: Packets are network-layer units (PDF 15, 16, 15, 14.)

D - Incorrect: Segments are transport-layer units (PDF 15, 16, 15, 14.)

Primary note proof

Study-note section NET12

> Sending proceeds from application data to transport segment/datagram, network packet, link frame and physical bits/symbols; receiving reverses the order. Each layer serves the layer above. A router removes a received link frame, inspects IP, and creates a new link frame for the next hop. MAC addresses usually change across routed hops; end-to-end IP addresses ordinarily remain until translation.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 15 | lines 13-40

> Data Link Layer
> • The Data Link layer adds reliability to the physical layer by providing error detection and correction mechanisms.
> • Framing: the Data Link layer receives the data from Network Layer and divides the stream of bits into fixed size manageable units called as Frames and sends it to the physical layer. On the receiver

side, the data link layer receives the stream of bits from the physical layer and regroups them into frames and sends them to the Network layer.
• Physical Addressing: The Data link layer appends the physical address in the header of the frame before sending it to physical layer.
• Flow control: The data link layer makes sure that the sender sends the data at a speed at which the receiver canreceive it else if there is an overflow at the receiver sidethe data will be lost.
• Error Control: The data link layer imposes error control mechanism to identify lost or damaged frames, duplicateframes and then retransmit them.
• Access Control: The data link layer imposes access control mechanism to determine which device has right to send data in an multipoint connection setting.
• Main Responsibility: The main responsibility of the data link layer is hop to hop transmission of frames.

Data Communication and Computer Networking module | PDF page 16 | lines 2-17

• At the sending side, the transport layer receives data from the session layer, divides it into units called segments and sends it to the network layer.
• To ensure process to process delivery the transport layer makes use of port address to identify the data from the sending and receiving process.
• The data can be transported in a connection oriented or connectionless manner.
• The Transport layer is responsible for segmentation and reassembly of the message into segments which bear sequence numbers.
• The transport layer also carries out flow control and error control functions; but unlike data link layer these are end to end rather than node to node.
• The main responsibility of the transport layer is process to process delivery of the entire message

Data Communication and Computer Networking module | PDF page 15 | lines 41-61

Network Layer
• The network layer makes sure that the data is deliveredto the receiver despite multiple intermediate devices.
• The network layer at the sending side accepts data from the transport layer, divides it into

packets, addsaddressing information in the header and passes it tothe data link layer.
• The network layer is responsible for source todestination of delivery of data.
• The network layer uses logical address commonlyknown as IP address to recognize devices on the network.
• Each packet is independent of the other and may travelusing different routes to reach the receiver hence may arrive out of turn at the receiver (Routing).
• The Network layer does not perform any flow controlor error control
• The main responsibility of Network Layer is transmission of packets from source to destination

Data Communication and Computer Networking module | PDF page 14 | lines 32-49

Physical Layer:
• The Physical Layer provides a standardized interface to physical transmission media, including: Mechanical specification of electrical connectors and cables, for example maximum cable length, Electrical specification of transmission line and Bit-by-bit or symbol-by-symbol delivery.
• Interface: The Physical Layer defines the characteristics of interfaces between the devices & transmission medium.
• Representation of bits: The physical layer is concerned with transmission of signals from one device to another which involves converting data (1_s & 0_s) into signals and vice versa. It is not concerned with the meaning or interpretation of bits.
• Data rate: The physical layer defines the data transmission rate i.e. number of bits sent per second. It is the responsibility of the physical layer to maintain the defined data rate.

Question sources

Computer Science model exam 2 · Question 50

Question 91 | Q01258

What is the maximum number of IP addresses that can be assigned to hosts on a local subnet that uses the 255.255.255.224 subnet mask?

A. 14

B. 32

C. 24

D. 30

Hint

Convert the mask to a prefix, separate network and host bits, and apply the relevant subnet-count or usable-host rule.

Answer D: 30 usable host addresses

The final mask octet 224 is 11100000, making the prefix /27 and leaving five host bits. There are 2^5=32 addresses in each block. For an ordinary broadcast subnet, one identifies the network and one the broadcast, leaving 30 assignable host addresses; total addresses must not be confused with usable hosts.

Why each choice is right or wrong

A - Incorrect: Fourteen usable hosts would correspond to /28, not this /27 mask.

B - Incorrect: Thirty-two is the total address count before reserving the network and broadcast addresses.

C - Incorrect: Twenty-four is not the usable count obtained from five host bits and two reservations.

D - Correct: Five host bits yield 32 total addresses minus two reserved addresses, leaving 30 hosts.

Primary note proof

Study-note section NET25

> For ordinary broadcast LANs let h=32-p. Total addresses=2^h; usable hosts=2^h-2, reserving network and directed broadcast. Find the changing octet's increment as 256-mask octet, round the address down to a multiple, and extend through the next boundary minus one.

Study-note section NET24

> A /p IPv4 prefix has p leading one bits followed by 32-p zeros. Partial octet masks are 128,192,224,240,248,252,254. /19 is 255.255.224.0; /20 is 255.255.240.0; /21 is 255.255.248.0, correcting the study guide's 255.248.0.0 mistake.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 19 | lines 2-22

Address Space: An address space is the total number ofaddresses used by the protocol.
• If a protocol uses N bits to define an address, the address space is 2N because each bit can have twodifferent values (0 or 1) and N bits can have 2N values.
• IPv4 uses 32-bit addresses, which means that the address space is 232 or 4,294,967,296 (more than 4billion).
Notations: There are two notations to show an IPv4 address:
• Binary notation: The IPv4 address is displayed as 32bits. ex. 11000001 10000011 00011011 11111111
• Dotted decimal notation: To make the IPv4 address easier to read, Internet addresses are usually written in decimal form with a decimal point (dot) separatingthe bytes. Each byte (octet) is 8 bits hence each number in dotted-decimal notation is a value rangingfrom 0 to 255. Ex. 129.11.11.239

Data Communication and Computer Networking module | PDF page 19 | lines 23-36

Classful addressing : In classful addressing, the addressspace is divided into five classes: A, B, C, D, and E.
• Netid and Hostid In classful addressing, an IP addressin class A, B, or C is divided into netid and hostid.
Subnetting: It allows a network to be split into several parts for internal use but still act like a single network to the outsideworld.
• To implement subnetting, the router needs a subnet mask that indicates the split between network + subnet number and host. Ex. 255.255.252.0/22. A‖/22‖ to indicate that the subnet mask is 22 bits long.

Question sources

Computer Science model exam 2 · Question 79

Question 92 | Q01270

Which one of the following is not LAN technologies?

A. Token Ring

B. Ethernet

C. X.25 or Frame Relay

D. None

Hint

Use the cited note definitions to identify the requested function or scope, then check each alternative against that same rule.

Answer C: X.25 or Frame Relay

The module explicitly contrasts LAN Ethernet/Token Ring with WAN X.25/Frame Relay. Evidence: PDF 26.

Why each choice is right or wrong

A - Incorrect: Token Ring is explicitly a LAN technology (PDF 26.)

B - Incorrect: Ethernet is explicitly a LAN technology (PDF 26.)

C - Correct: X.25 and Frame Relay are explicitly WAN technologies (PDF 26.)

D - Incorrect: None fails because the WAN pair is present (PDF 26.)

Primary note proof

Study-note section NET-S05

> Ethernet and Token Ring are traditional LAN technologies. X.25 and Frame Relay are traditional WAN technologies. TCP/IP can run over different network-access technologies; its Internet-layer packet service does not require one particular link medium or frame format.

Study-note section NET31

> Circuit switching sets up a path with reserved resources, transfers data, then releases it. Predictable allocated bandwidth trades against setup/blocking and wasted reservation during silence. A traditional telephone call is the standard example. Packet switching divides data into packets that share links statistically; queueing can add variable delay and loss. This does not make modern voice-over-packet impossible: buffering, scheduling and capacity planning manage it.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 26 | lines 14-28

> medium. TCP/IP was designed to be independent
> of the network access method, frame format, and
> medium. In this way, TCP/IP can be used to

connect differing network types. These include LAN technologies such as Ethernet and Token Ring and WAN technologies such as X.25 and Frame Relay. Independence from any specific network technology gives TCP/IP the ability to be adapted to new technologies such as Asynchronous Transfer Mode (ATM).
Network Access layer uses a physical address to identify hosts and to deliver data.
The Network Access layer PDU is called a frame. It contains the IP packet as well as a protocol header and trailer from this layer.

Question sources

Computer Science model exam 2 · Question 91

Question 93 | Q01276

Which internet layer address is responsible for providing diagnostic functions and reporting errors or conditions regarding the delivery of IP packets?

A. Internet Protocol (IP)

B. Address Resolution Protocol (ARP)

C. Internet Control Message Protocol (ICMP)

D. Internet Group Message Protocol (IGMP)

Hint

Match the requested scope or data unit to the layer duties in the note; distinguish hop delivery from end-to-end process delivery.

Answer C: Internet Control Message Protocol (ICMP)

ICMP reports transit problems and supports destination-unreachable, echo and timeout diagnostics. The stem calls it an address, but asks for a protocol by its functions. Evidence: PDF 17, 27, 17, 17.

Why each choice is right or wrong

A - Incorrect: IP supplies best-effort datagram delivery (PDF 17, 27, 17, 17.)

B - Incorrect: ARP resolves IP to hardware address (PDF 17, 27, 17, 17.)

C - Correct: ICMP explicitly provides error/diagnostic messages (PDF 17, 27, 17, 17.)

D - Incorrect: IGMP supports group recipients rather than these transit diagnostics (PDF 17, 27, 17, 17.)

Primary note proof

Study-note section NET20

ARP resolves an on-link IPv4 next hop to a link address, using a broadcast request and normally unicast reply. For an off-subnet target, ARP resolves the gateway, not the remote target's MAC. It bridges the network/link addressing boundary and is often classified at the link layer; calling ARP simply a network protocol uses a loose textbook convention. RARP reverses hardware-to-IP lookup; BOOTP/DHCP support boot configuration. ICMP reports errors and diagnostics; IGMP manages IPv4 multicast membership. These are separate companion protocols, not four pieces whose combination is IP.

Study-note section NET16

IP supplies connectionless best-effort packet delivery, not end-to-end ordering or retransmission. IPv4 addresses are 32 bits. Its minimum header is 20 bytes and can grow to 60 bytes; it is not a 32-bit header. IHL counts 32-bit words; total length includes header and payload. TTL limits lifetime across routers; the protocol field identifies TCP, UDP or another upper-layer protocol.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 17 | lines 54-59

ICMP- Internet Control Message Protocol: It is a
signaling mechanism used to inform the sender about
datagram problemsthat occur during transit. It is used by
intermediate devices.
IGMP- Internet Group Message Protocol: It is a mechanism
that allows sending the same message to a group of recipients.

Data Communication and Computer Networking module | PDF page 27 | lines 5-31

Internet Control Message Protocol (ICMP):
works at the Network layer and is used by IP for
many different services. ICMP is a management
protocol and messagingservice provider for IP. The
following are some common events and messages
that ICMP relates to:
Destination Unreachable: If a router can‘t send an
IP datagram any further, it uses ICMP to send a
message back to the sender, advising it of the
situation.
Buffer Full: If a router‘s memory buffer for
receiving incoming datagrams is full, it will use
ICMP to send out this message until the congestion
abates.
Hops: Each IP datagram is allotted a certain number
of routers, called hops, to pass through. If it reaches
its limitof hops before arriving at its destination, the
last router to receive that datagram deletes it. The

executioner router then uses ICMP to send an obituary message, informing the sending machine of the demise of its datagram.
Ping (Packet Internet Groper) uses ICMP echo messages to check the physical and logical connectivity of machineson a network.
Traceroute Using ICMP timeouts, Traceroute is used to discover the path a packet takes as it traverses an Internetwork.

Data Communication and Computer Networking module | PDF page 17 | lines 44-53

ARP - Address Resolution Protocol: It is used to resolve thephysical address of a device on a network, where its logical address is known.
Physical address is the 48 bit address that is imprinted on theNIC or LAN card, Logical address is the Internet Address orcommonly known as IP address that is used to uniquely & universally identify a device.
RARP- Reverse Address Resolution Protocol: It is used bya device on the network to find its Internet address when it knows its physical address.

Data Communication and Computer Networking module | PDF page 17 | lines 22-38

Network Layer or IP
Also called as the Internetwork Layer (IP). It holds the IP protocol which is a network layer protocol and is responsiblefor source to destination transmission of data.
The Internetworking Protocol (IP) is a connection-less & unreliable protocol.
It is a best effort delivery service. i.e. there is no error checking in IP, it simply sends the data and relies on its underlying layers to get the data transmitted to the destination.Even if it is unreliable IP cannot be considered weak and useless; since it provides only the functionality that is requiredfor transmitting data thereby giving maximum efficiency.
Since there is no mechanism of error detection or correction in IP, there will be no delay introduced on a medium where thereis no error at all.

Question sources

Computer Science model exam 2 · Question 97

Question 94 | Q01277

Hana divides a 172.16.0.0/16 parent into equal /19 broadcast subnets. Counting every subnet, which option correctly gives the subnet count and usable hosts per subnet?

A. 7 subnets and 30 valid hosts

B. 8 subnets and 8190 usable hosts in each subnet

C. 8 subnets and 2046 valid hosts in each subnet

D. 7 subnets and 2046 valid hosts in each subnet

Hint

Convert the mask to a prefix, separate network and host bits, and apply the relevant subnet-count or usable-host rule.

Answer B: 8 subnets and 8190 usable hosts in each subnet

The /16-to-/19 subdivision borrows three bits, so it creates eight equal subnets. Each /19 leaves thirteen host bits, producing 8192 total addresses and 8190 usable hosts after network and broadcast reservations. Modern counting includes every subnet. The option changes only the obsolete subnet count; the calculation still requires distinguishing child subnet count from host capacity.

Why each choice is right or wrong

A - Incorrect: Neither seven subnets nor thirty usable hosts follows from /19; thirty hosts would require /27.

B - Correct: Three subnet bits give eight subnets and thirteen host bits give 8190 usable hosts.

C - Incorrect: Eight subnets is correct for the stated /16 parent, but a /19 has 8190 usable hosts rather than 2046.

D - Incorrect: Seven lacks a stated counting basis, and 2046 hosts corresponds to /21 rather than /19.

Primary note proof

Study-note section NET26

> To split parent /a into equal /p blocks, borrow b=p-a bits and obtain 2^b subnets. Do not subtract two subnets under modern practice. For a Class B /16 parent split to /19, b=3 gives eight subnets, each with 8192 addresses and 8190 conventional hosts. A /19 alone does not state its parent.

Study-note section NET25

> For ordinary broadcast LANs let h=32-p. Total addresses=2^h; usable hosts=2^h-2, reserving network and directed broadcast. Find the changing octet’s increment as 256-mask octet, round the address down to a multiple, and extend through the next boundary minus one.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 18 | lines 45-54

IP addresses: IP address uniquely identifies a device on the Internet. Every host and router on the Internet has an IP address, which encodes its network number and host number.
• The combination is unique: in principle, no two machines on the Internet have the same IP address.
• An IPv4 address is 32 bits long
• They are used in the Source address and Destination address fields of IP packets.
• An IP address does not refer to a host but it refers to a network interface.

Data Communication and Computer Networking module | PDF page 19 | lines 2-22

Address Space: An address space is the total number ofaddresses used by the protocol.
• If a protocol uses N bits to define an address, the address space is 2N because each bit can have twodifferent values (0 or 1) and N bits can have 2N values.
• IPv4 uses 32-bit addresses, which means that the address space is 232 or 4,294,967,296 (more than 4billion).
Notations: There are two notations to show an IPv4 address:
• Binary notation: The IPv4 address is displayed as 32bits. ex. 11000001 10000011 00011011 11111111
• Dotted decimal notation: To make the IPv4 address easier to read, Internet addresses are usually written in decimal form with a decimal point (dot) separatingthe bytes. Each byte (octet) is 8 bits hence each number in dotted-decimal notation is a value rangingfrom 0 to 255. Ex. 129.11.11.239

Data Communication and Computer Networking module | PDF page 19 | lines 23-36

Classful addressing : In classful addressing, the addressspace is divided into five classes: A, B, C, D, and E.
• Netid and Hostid In classful addressing, an IP addressin class A, B, or C is divided into netid and hostid.
Subnetting: It allows a network to be split into several parts for internal use but still act like a single network to the outsideworld.
• To implement subnetting, the router needs a subnet mask that indicates the split between network + subnet number and host. Ex.

255.255.252.0/22. A‖/22‖ to indicate that the subnet mask is 22 bits long.

Question sources

Computer Science model exam 2 · Question 98

Question 95 | Q01494

A switch-based LAN is more efficient than a hub-based LAN because:

A. A switch can connect two different LANs together

B. A switch allows multiple computers to send at the same time

C. A hub uses reservation-based MAC protocols

D. A switch uses contention-based MAC protocols

E. A switch is easier to implement than a hub.

Hint

Compare signal repetition, frame forwarding, packet routing and policy enforcement using the stated device or traffic assumptions.

Answer B: A switch allows multiple computers to send at the same time

Switches direct frames toward the MAC recipient instead of copying all traffic to every port. Independent point-to-point communication permits multiple simultaneous exchanges on suitable separate ports. Evidence: PDF 12, 12.

Why each choice is right or wrong

A - Incorrect: Connecting LANs is not the efficiency distinction in the switch/hub comparison (PDF 12, 12.)

B - Correct: Selective independent port communication explains the improvement (PDF 12, 12.)

C - Incorrect: The module says hubs repeat/broadcast, not reservation-based MAC (PDF 12, 12.)

D - Incorrect: A switch is not defined by a contention-based MAC distinction from hubs (PDF 12, 12.)

E - Incorrect: The module calls switches more intelligent and expensive, not easier to implement (PDF 12, 12.)

Primary note proof

Study-note section NET10

A bridge or ordinary Ethernet switch operates at layer 2. It learns source-MAC-to-port mappings, looks up the destination, forwards a known unicast to its port, filters it if the destination is on the incoming segment, and floods an unknown unicast or broadcast within its VLAN. A switch does

not always send only to one destination port. Wireless access points normally bridge wireless and wired link-layer traffic.

Study-note section NET10

Each switch port separates collision domains; full-duplex point-to-point Ethernet has no collisions and does not use CSMA/CD. Switching permits independent conversations simultaneously. Broadcasts still reach the VLAN unless another control filters them. A layer-3 switch also routes, so device marketing names do not override the function being examined.

Study-note section NET09

A repeater regenerates layer-1 signals without inspecting destination addresses. An active hub is a multiport repeater: it repeats incoming signals onto other ports, placing half-duplex endpoints in one collision domain. A passive hub is a connector. A hub neither learns MAC addresses nor eliminates collisions. An endpoint such as a network printer consumes services; routers, hubs and access points are intermediary devices.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 12 | lines 27-37

SWITCH: A switch filters and forwards data packets
across anetwork.
Unlike a hub which simply replicates what it receives on
oneport onto all the other ports, a switch keeps a record
of the MAC addresses of the devices attached to it.
When the switch receives a data packet, it forwards the
packetdirectly to the recipient device by looking up the
MAC address.
• Switch is intelligent and expensive than Hub
• Switch is a point to point communication device
• Hub is a broadcasting device

Data Communication and Computer Networking module | PDF page 12 | lines 17-26

Active Hubs
An active hub is actually a multipart repeater. It is
normallyused to create connections between stations in
a physical startopology.
HUB: Hubs are commonly used to connect segments
(devices)of a LAN. Hubs don‘t filter information; instead
broadcast incoming packets to all computers connected to
it. A hub contains multiple ports which support 8, 12 or
24 RJ-45 ports. Two types: Passive hub and Active hub. It
is used in star or ring topology.

Question sources

Mock exam 1 · Question 10

Question 96 | Q01496

Compare circuit switching versus datagram packet switching. An advantage of circuit switching is it:

A. Allows end hosts to use different line rates.

B. Can guarantee the performance delivered to end hosts.

C. Establishes a connection before sending data.

D. Sends packets instead of signals.

E. Is non-blocking.

F. Is efficient when the amount of traffic to be sent by end hosts varies over time.

Hint

Compare signal repetition, frame forwarding, packet routing and policy enforcement using the stated device or traffic assumptions.

Answer B: Reserved resources can guarantee performance

The reserved-resource circuit supports predictable allocated bandwidth and performance, the advantage contrasted with datagram links shared statistically. Establishing a connection is a procedural characteristic and imposes setup cost rather than itself guaranteeing a benefit. The note explicitly identifies blocking and wasted reservation during silence, ruling out the nonblocking and variable-traffic-efficiency claims.

Why each choice is right or wrong

A - Incorrect: Different endpoint line rates are not the reserved-circuit advantage established in the note.

B - Correct: Reserved resources provide predictable allocated bandwidth and can guarantee the agreed performance to endpoints.

C - Incorrect: Setup is a characteristic of circuit operation, but is not itself the performance advantage requested.

D - Incorrect: Circuit switching establishes reserved resources; packet-versus-signal wording does not describe its advantage.

E - Incorrect: NET31 explicitly identifies blocking as a circuit-switching tradeoff.

F - Incorrect: Reservations can be wasted during silence, making highly variable traffic less efficient on fixed circuits.

Primary note proof

Study-note section NET31

> Circuit switching sets up a path with reserved resources, transfers data, then releases it. Predictable allocated bandwidth trades against setup/blocking and wasted reservation during silence. A traditional telephone call is the standard example. Packet switching divides data into

packets that share links statistically; queueing can add variable delay and loss. This does not make modern voice-over-packet impossible: buffering, scheduling and capacity planning manage it.

Study-note section NET31

Datagram packets are forwarded independently. Virtual circuits establish forwarding state, but resource reservation is optional, not a necessary property of every virtual circuit. Message switching stores a complete message before forwarding, without a dedicated end-to-end path. Packet store-and-forward waits for the full packet/frame; cut-through starts after enough header arrives; fragment-free historically waits through the initial collision-sensitive portion. No routing algorithm guarantees that every packet always takes the geometrically shortest route.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 20 | lines 12-26

Circuit Switching: In circuit switching, two communicating stations are connected by a dedicated communication path which consists of intermediate nodes in the network and the links that connect these nodes.
It involved the following three distinct steps
• Circuit Establishment: To establish an end-to-end connection before any transfer of data.
• Data transfer: Transfer data is from the source to the destination. The data may be analog or digital, depending on the nature of the network. The connection is generally full-duplex.
• Circuit disconnect: Terminate connection at the end of data transfer. Signals must be propagated to deallocate the dedicated resources.

Data Communication and Computer Networking module | PDF page 20 | lines 27-36

Message Switching:
Packet Switching: Packet switching was designed to address the shortcomings of circuit switching in dealing with data communication. Unlike circuit switching where communication is continuous along a dedicated circuit, in packet switching, communication is discrete in form of packets.
The three switching modes to choose from are:
• Cut-through
• Store-and-forward
• Fragment-free

Question sources

Mock exam 1 · Question 12

Question 97 | Q01521

A _____ is a system in which multiple computers are connected to each other to share information and resources.

A. Hardware

B. Software

C. Number system

D. Computer network

Hint

Use the cited note definitions to identify the requested function or scope, then check each alternative against that same rule.

Answer D: Computer network

The module defines a network as connected computers sharing resources and exchanging information. Evidence: PDF 22.

Why each choice is right or wrong

A - Incorrect: Hardware alone need not connect computers for sharing (PDF 22.)

B - Incorrect: Software alone is not the system of connected devices (PDF 22.)

C - Incorrect: A number system is a representation scheme, not shared computers (PDF 22.)

D - Correct: Computer network matches the supplied definition (PDF 22.)

Primary note proof

Study-note section NET-S04

> A computer network connects computers or other devices so they can exchange information and share resources such as files, storage and printers. The interconnection uses both hardware and software; neither hardware alone nor software alone is the definition of the whole network.

Study-note section NET02

> An intranet serves an organization internally; an extranet exposes selected services to approved outsiders. Neither term alone specifies geographic size. A client requests a service; a server supplies it. Peer systems may perform both roles. Dedicated servers concentrate on service workloads but can still be clients of DNS, backup or update services. A ten-user cutoff is a teaching guideline, not a technical law. Centralization simplifies administration but creates dependencies; peer networks still need security.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 22 | lines 2-19

A network can be defined as two or more computers connected together in such a way that they can share resources. The primary purpose of a network is to share resources, and a resource could be:
• a file,
• a folder,
• a printer,
• a disk drive, or just about anything else that exists on a computer.
Therefore, a computer network is simply a collection of computers or other hardware devices that are connected together, either physically or logically, using special hardware and software, to allow them to exchange information and cooperate. Networking is the term that describes the processes involved in designing, implementing, upgrading, managing and otherwise working with networks and network technologies.

Question sources

Data Communication & Networking practice questions · Question 1

Question 98 | Q01522

NIC stands for?

A. Network Internal Card

B. Network Interconnect Card

C. Network Interface Card

D. Network Interface Component

Hint

Find the full expansion in the terminology note and compare each word rather than only matching initials.

Answer C: Network Interface Card

The star cabling paragraph explicitly expands NIC as Network Interface Card. Evidence: PDF 23.

Why each choice is right or wrong

A - Incorrect: Internal differs from the printed Interface (PDF 23.)

B - Incorrect: Interconnect differs from the printed Interface (PDF 23.)

C - Correct: Exact expansion is Network Interface Card (PDF 23.)

D - Incorrect: Component differs from the printed Card (PDF 23.)

Primary note proof

Study-note section NET-S04

NIC expands to Network Interface Card. It is the host's network interface, providing the connection through which the host sends and receives network signals. A cable connector attaches the medium to that interface; it is distinct from an intermediary switch or router.

Study-note section NET09

A NIC supplies a computer's network interface and commonly implements both physical and link functions. Calling a NIC a physical interface does not mean all its functions are layer 1. Physical specifications include connectors, signaling, voltage, timing and physical coding/modulation; the PHY interface to MAC handles hardware signaling.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 23 | lines 19-34

Star Topology: in this topology, each node is connected directly to a central device called a hub or a switch. Data on a star network passes through the central device (switch) before continuing to its destination. The central device manages and controls all functions of the network. This configuration is common with twisted pair cable. RJ-45 Connectors are used to connect the cable to the Network Interface Card (NIC) of each computer. Its advantages include, ease of installation and reconfiguration, robust (ease of fault identification and isolation), link failure only affects device(s) connected to that link, and is less expensive than mesh. Its drawbacks include more cable requirements (than bus and ring) and single point of failure (if central device fail, the whole system will be down).

Question sources

Data Communication & Networking practice questions · Question 2

Question 99 | Q01523

A term that refers to the way in which the nodes of a network are linked together.

A. network

B. topology

C. connection

D. interconnectivity

Hint

Use the cited note definitions to identify the requested function or scope, then check each alternative against that same rule.

Answer B: topology

Topology is explicitly the shape/layout and relation among links and devices, matching the way nodes are linked. Evidence: PDF 22, 11.

Why each choice is right or wrong

A - Incorrect: Network is the collection of devices, not the specific arrangement term (PDF 22, 11.)

B - Correct: Topology is the defined arrangement term (PDF 22, 11.)

C - Incorrect: Connection is a generic link rather than the named layout concept (PDF 22, 11.)

D - Incorrect: Interconnectivity is the organizing attribute, while topology names its layout (PDF 22, 11.)

Primary note proof

Study-note section NET08

> Physical topology describes link layout; logical topology describes communication/access relationships. Point-to-point links join two endpoints; multipoint links share a medium. A full mesh consists of point-to-point links.

Study-note section NET08

> Bus uses a shared backbone; an unterminated break can disrupt the segment. Star connects endpoints through a central device: one edge failure isolates that endpoint, whereas central failure affects the star. Ring forms a loop; basic single rings are vulnerable to a break, while protected dual rings differ. Token passing is associated with Token Ring but is an access method, not a necessary property of every ring. Tree is hierarchical; hybrid combines arrangements.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 22 | lines 45-52

> Inter-connectivity: components of a network,
> including end devices and interconnecting devices,
> can be connected to each other differently in some
> fashion. By connectedness we mean either logically,
> physically or both ways. Network topology refers to
> the shape of a network, or the network‘s layout. It is
> the geometric representation of the relationship of all
> the links and linking devices to one another. There are

Data Communication and Computer Networking module | PDF page 11 | lines 34-51

> NETWORK TOPOLOGY
> A network topology is a description of the layout of the region

or area covered by that network.
There are two types of connections. They are: point-to-point and multi-point.
Point-to-point connections provide a direct link between two devices.
Multi-point connections provide a link between three or more devices on a network.
There are seven basic topologies in the study of network topology:
• Point-to-point topology,
• Bus (point-to-multipoint) topology,
• Ring topology,
• Star topology,
• Hybrid topology,
• Mesh topology and,
• Tree topology.

Question sources

Data Communication & Networking practice questions · Question 3

Question 100 | Q01524

A topology that involves Tokens.

A. Star

B. Bus

C. Ring

D. Daisy Chaining

Hint

Draw the links and identify shared components, alternate paths and the effect of the specified failure or growth requirement.

Answer C: Ring in the conventional Token Ring association

NET08 associates token passing with Token Ring, so ring is the intended topology among these choices. The answer is an association rather than a universal claim: token passing is an access method and not every ring must use it. None of the other topology names inherently establishes token access.

Why each choice is right or wrong

A - Incorrect: A star describes central connections and does not itself specify token access.

B - Incorrect: A bus describes a shared backbone; token access is not inherent in that layout.

C - Correct: Token Ring is the conventional association, with the caveat that tokens are an access method.

D - Incorrect: Daisy chaining describes successive connections and does not by itself establish token passing.

Primary note proof

Study-note section NET08

Bus uses a shared backbone; an unterminated break can disrupt the segment. Star connects endpoints through a central device: one edge failure isolates that endpoint, whereas central failure affects the star. Ring forms a loop; basic single rings are vulnerable to a break, while protected dual rings differ. Token passing is associated with Token Ring but is an access method, not a necessary property of every ring. Tree is hierarchical; hybrid combines arrangements.

Study-note section NET14

Controlled access uses polling, reservations or a token to grant turns; correctly coordinated access avoids contention collisions. Channelization divides frequency, time or code resources. Stop-and-wait sends one frame and waits for ACK, retransmitting on timeout; sequence bits distinguish duplicates. Sliding windows permit multiple unacknowledged frames. Link reliability/flow control is hop-local; transport reliability/flow control is end-to-end. Ethernet detects corruption but does not itself guarantee reliable delivery.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 21 | lines 6-26

MEDIUM ACCESS CONTROL
The problem of controlling the access to the medium is similarto the rules of speaking in a meeting (the right to speak isupheld; two people do not speak at the same time; do notinterrupt each other; do not monopolize the discussion; ...) Three categories of multiple access protocols
Random Access Protocols - try your best like taxis do
• MA - Multiple Access
• CSMA - Carrier Sense MA
• CSMA/CD - CSMA with Collision Detection
• CSMA/CA - CSMA with Collision AvoidanceControlled-Access Protocols - get permission
• Reservation
• Polling
• Token Passing
Channelization Protocols - simultaneous use
• FDMA - Frequency-Division MA
• TDMA - Time-Division MA
• CDMA - Code-Division MA

Data Communication and Computer Networking module | PDF page 23 | lines 35-44

> Ring Topology: in this topology, all devices are connected to one another in the shape of a closed loop, so that each device is connected directly to two other devices, one on either side of it. Some of its advantages include, easy to install and reconfigure, less expensive (than mesh), and performance is even despite the number of users. Its cons include, break in the ring (such as a disabled station) can disable the entire network, and limitations on media and traffic (limitation on ring length and number of devices).

Question sources

Data Communication & Networking practice questions · Question 4

Question 101 | Q01525

Physical or logical arrangement of network is _____

A. Topology

B. Routing

C. Networking

D. Control

Hint

Use the cited note definitions to identify the requested function or scope, then check each alternative against that same rule.

Answer A: Topology

Physical or logical relations among links and devices form the network topology; routing chooses paths over that arrangement. Evidence: PDF 22, 19.

Why each choice is right or wrong

A - Correct: Topology is explicitly the arrangement/layout

B - Incorrect: Routing chooses a packet path, not the whole arrangement

C - Incorrect: Networking includes designing and managing networks broadly

D - Incorrect: Control does not name the defined arrangement

Primary note proof

Study-note section NET08

> Physical topology describes link layout; logical topology describes communication/access relationships. Point-to-point links join two endpoints; multipoint links share a medium. A full mesh consists of point-to-point links.

Study-note section NET30

Routing computes paths; forwarding chooses a next hop for an individual packet. Select the matching route with the longest prefix, then apply the routing system's tie-breaking criteria. A default /0 matches when nothing more specific does. Static routes are configured; dynamic protocols exchange reachability. Distance vector uses neighbor estimates, while link state distributes link information and computes shortest paths. Interior protocols operate within an autonomous system; BGP exchanges routes between systems.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 22 | lines 45-52

Inter-connectivity: components of a network,
including end devices and interconnecting devices,
can be connected to each other differently in some
fashion. By connectedness we mean either logically,
physically or both ways. Network topology refers to
the shape of a network, or the network‘s layout. It is
the geometric representation of the relationship of all
the links and linking devices to one another. There are

Data Communication and Computer Networking module | PDF page 19 | lines 52-64

ROUTING AND ROUTING PROTOCOLS
Routing is the act of moving information across an
internetwork from a source to a destination. At the heart of
such protocol is the routing algorithm that determines the
path for a packet.
• Routing requires a host or a router to have a
routingtable which is constructed by the routing
algorithm.
• There are wo kinds of routing algorithms (routing
tables): nonadaptive (static) and adaptive (dynamic)
• And two kinds of protocols
o Interior routing protocols
o Exterior routing protocols

Question sources

Data Communication & Networking practice questions · Question 5

Question 102 | Q01526

Which network topology requires a central controller or hub?

A. Star

B. Mesh

C. Ring

D. Bus

Hint

Draw the links and identify shared components, alternate paths and the effect of the specified failure or growth requirement.

Answer A: Star

Star explicitly connects each node to a central hub or switch. Mesh, ring and bus have different connection structures. Evidence: PDF 23, 23, 23, 23.

Why each choice is right or wrong

A - Correct: Central hub/switch is the defining star feature (PDF 23, 23, 23, 23.)

B - Incorrect: Full mesh uses all-pairs links (PDF 23, 23, 23, 23.)

C - Incorrect: Ring connects two neighbors per node (PDF 23, 23, 23, 23.)

D - Incorrect: Bus uses a common backbone rather than a controller (PDF 23, 23, 23, 23.)

Primary note proof

Study-note section NET08

> Bus uses a shared backbone; an unterminated break can disrupt the segment. Star connects endpoints through a central device: one edge failure isolates that endpoint, whereas central failure affects the star. Ring forms a loop; basic single rings are vulnerable to a break, while protected dual rings differ. Token passing is associated with Token Ring but is an access method, not a necessary property of every ring. Tree is hierarchical; hybrid combines arrangements.

Study-note section NET08

> A full undirected mesh of n nodes needs n(n-1)/2 links and n-1 interfaces per node. For 50 nodes: 50×49/2=1225 links. Redundant paths improve fault tolerance at greater cable and interface cost.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 23 | lines 19-34

> Star Topology: in this topology, each node is
> connected directly to a central device called a hub or
> a switch. Data on a star network passes through the
> central device (switch) before continuing to its
> destination. The central device manages and controls

all functions of the network. This configuration is common with twisted pair cable. RJ-45 Connectors are used to connect the cable to the Network Interface Card (NIC) of each computer. Its advantages include, ease of installation and reconfiguration, robust (ease of fault identification and isolation), link failure only affects device(s) connected to that link, and is less expensive than mesh. Its drawbacks include more cable requirements (than bus and ring) and single point of failure (if central device fail, the whole system will be down).

Data Communication and Computer Networking module | PDF page 23 | lines 45-53

Mesh Topology: in this topology devices are connected with many redundant interconnections between network nodes. In a full mesh topology, every node has a connection to every other node in the network, which makes it the most expensive topology over all the other topologies. The number of cables grows fast as the number of nodes increases, and it can be calculated by using the general formula ((n (n - 1)) /2), where n is the number of nodes in the

Data Communication and Computer Networking module | PDF page 23 | lines 35-44

Ring Topology: in this topology, all devices are connected to one another in the shape of a closed loop, so that each device is connected directly to two other devices, one on either side of it. Some of its advantages include, easy to install and reconfigure, less expensive (than mesh), and performance is even despite the number of users. Its cons include, break in the ring (such as a disabled station) can disable the entire network, and limitations on media and traffic (limitation on ring length and number of devices).

Data Communication and Computer Networking module | PDF page 23 | lines 4-18

Bus Topology: in this topology all devices are connected to a central cable, called the bus or backbone, which is terminated at its ends. The purpose of the terminators is to stop the signal from bouncing, thereby clearing the cable so that other computers can send data. Message transmitted along the Bus is visible to all computers connected to the backbone cable. As the message arrives at each workstation, the workstation checks the destination address contained in the message either to process or

drop the packet if it matches or not respectively. Its advantages are, ease of installation and less amount of cable requirement. Its main drawback is, the entire network will be shut down if there is a break in the main cable.

Question sources

Data Communication & Networking practice questions · Question 6

Question 103 | Q01527

_____ topology requires a multipoint connection.

A. Star

B. Mesh

C. Ring

D. Bus

Hint

Draw the links and identify shared components, alternate paths and the effect of the specified failure or growth requirement.

Answer D: Bus uses a shared multipoint backbone

A multipoint connection shares one medium among endpoints. NET08 describes bus as a shared backbone, while a full mesh consists of separate point-to-point links. Ordinary star and ring link layouts connect endpoints through separate adjacent links rather than requiring a common shared bus. D is therefore the topology matching multipoint sharing.

Why each choice is right or wrong

A - Incorrect: A star connects endpoints through a central device using individual edge links rather than requiring a shared backbone.

B - Incorrect: A full mesh consists of point-to-point links, explicitly correcting the old contradictory multipoint claim.

C - Incorrect: A ring forms successive neighboring links, not the common shared backbone requested.

D - Correct: A bus shares one backbone among multiple endpoints, matching a multipoint connection.

Primary note proof

Study-note section NET08

Physical topology describes link layout; logical topology describes communication/access relationships. Point-to-point links join two endpoints; multipoint links share a medium. A full mesh consists of point-to-point links.

Study-note section NET08

Bus uses a shared backbone; an unterminated break can disrupt the segment. Star connects endpoints through a central device: one edge failure isolates that endpoint, whereas central failure affects the star. Ring forms a loop; basic single rings are vulnerable to a break, while protected dual rings differ. Token passing is associated with Token Ring but is an access method, not a necessary property of every ring. Tree is hierarchical; hybrid combines arrangements.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 11 | lines 34-51

NETWORK TOPOLOGY
A network topology is a description of the layout of the region or area covered by that network.
There are two types of connections. They are: point-to-point and multi-point.
Point-to-point connections provide a direct link between two devices.
Multi-point connections provide a link between three or more devices on a network.
There are seven basic topologies in the study of network topology:
• Point-to-point topology,
• Bus (point-to-multipoint) topology,
• Ring topology,
• Star topology,
• Hybrid topology,
• Mesh topology and,
• Tree topology.

Data Communication and Computer Networking module | PDF page 23 | lines 4-18

Bus Topology: in this topology all devices are connected to a central cable, called the bus or backbone, which is terminated at its ends. The purpose of the terminators is to stop the signal from bouncing, thereby clearing the cable so that other computers can send data. Message transmitted along the Bus is visible to all computers connected to the backbone cable. As the message arrives at each workstation, the workstation checks the destination address contained in the message either to process or drop the packet if it matches or not respectively. Its advantages are, ease of installation and less amount

of cable requirement. Its main drawback is, the entire network will be shut down if there is a break in the main cable.

Data Communication and Computer Networking module | PDF page 23 | lines 19-34

Star Topology: in this topology, each node is connected directly to a central device called a hub or a switch. Data on a star network passes through the central device (switch) before continuing to its destination. The central device manages and controls all functions of the network. This configuration is common with twisted pair cable. RJ-45 Connectors are used to connect the cable to the Network Interface Card (NIC) of each computer. Its advantages include, ease of installation and reconfiguration, robust (ease of fault identification and isolation), link failure only affects device(s) connected to that link, and is less expensive than mesh. Its drawbacks include more cable requirements (than bus and ring) and single point of failure (if central device fail, the whole system will be down).

Data Communication and Computer Networking module | PDF page 23 | lines 45-53

Mesh Topology: in this topology devices are connected with many redundant interconnections between network nodes. In a full mesh topology, every node has a connection to every other node in the network, which makes it the most expensive topology over all the other topologies. The number of cables grows fast as the number of nodes increases, and it can be calculated by using the general formula ((n (n - 1)) /2), where n is the number of nodes in the

Question sources

Data Communication & Networking practice questions · Question 7

Question 104 | Q01528

Data communication system spanning states, countries, or the whole world is _____

A. LAN

B. WAN

C. MAN

D. PAN

Hint

Use the cited note definitions to identify the requested function or scope, then check each alternative against that same rule.

Answer B: WAN

WAN explicitly spans multiple cities, countries, continents or the world. Evidence: PDF 22.

Why each choice is right or wrong

A - Incorrect: LAN is building/local organization span (PDF 22.)

B - Correct: WAN matches states/countries/world scale (PDF 22.)

C - Incorrect: MAN covers a city (PDF 22.)

D - Incorrect: PAN covers a few meters (PDF 22.)

Primary note proof

Study-note section NET02

PAN connects personal devices, such as Bluetooth accessories. LAN covers a local building or campus; MAN spans a metropolitan region; WAN connects distant regions. Device count alone does not determine the category. The Internet is a global network of networks, commonly the largest example of a WAN.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 22 | lines 26-44

Personal Area Network (PAN): is a network may be spanned across a given table with distances between the devices not more than few meters. The technology used to interconnect the devices could be a Bluetooth. These networks are called Personal Area Networks, since the devices interconnected in these networks are belongs to a single person.
Local Area Network (LAN): is a network that may span across a building, or across several buildings within a single organization, by using intermediate devices, like switches and/or hubs, to interconnect devices in all floors.
Metropolitan Area Network (MAN): is a network that may span across a whole city interconnecting several buildings and organizations.
Wide Area Network (WAN): is a network that may span across multiple cities, or an entire country, or an entire continent or it may even cover the whole world. For example, an Internet is one example of WAN.

Question sources

Data Communication & Networking practice questions · Question 8

Question 105 | Q01529

Data communication system within a building or campus is_____

A. LAN

B. WAN

C. MAN

D. PAN

Hint

Use the cited note definitions to identify the requested function or scope, then check each alternative against that same rule.

Answer A: LAN

A LAN can span a building or several buildings within an organization, fitting the intended single-campus scale. Evidence: PDF 22.

Why each choice is right or wrong

A - Correct: LAN matches the described building/campus extent (PDF 22.)

B - Incorrect: WAN spans cities or beyond (PDF 22.)

C - Incorrect: MAN spans a city (PDF 22.)

D - Incorrect: PAN is a few-meter personal range (PDF 22.)

Primary note proof

Study-note section NET02

> PAN connects personal devices, such as Bluetooth accessories. LAN covers a local building or campus; MAN spans a metropolitan region; WAN connects distant regions. Device count alone does not determine the category. The Internet is a global network of networks, commonly the largest example of a WAN.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 22 | lines 26-44

> Personal Area Network (PAN): is a network may be spanned across a given table with distances between the devices not more than few meters. The technology used to interconnect the devices could be a Bluetooth. These networks are called Personal Area Networks, since the devices interconnected in these networks are

belongs to a single person.
Local Area Network (LAN): is a network that may span across a building, or across several buildings within a single organization, by using intermediate devices, like switches and/or hubs, to interconnect devices in all floors.
Metropolitan Area Network (MAN): is a network that may span across a whole city interconnecting several buildings and organizations.
Wide Area Network (WAN): is a network that may span across multiple cities, or an entire country, or an entire continent or it may even cover the whole world. For example, an Internet is one example of WAN.

Question sources

Data Communication & Networking practice questions · Question 9

Question 106 | Q01530

Bluetooth is an example of _____

A. personal area network

B. local area network

C. virtual private network

D. wide area network

Hint

Use the cited note definitions to identify the requested function or scope, then check each alternative against that same rule.

Answer A: personal area network

The PAN definition explicitly gives Bluetooth as the interconnection technology for a few-meter personal network. Evidence: PDF 22.

Why each choice is right or wrong

A - Correct: PAN is the explicit Bluetooth example (PDF 22.)

B - Incorrect: LAN is building scale, not the cited Bluetooth example (PDF 22.)

C - Incorrect: VPN is not the geographic class in the example (PDF 22.)

D - Incorrect: WAN is much wider than the personal example (PDF 22.)

Primary note proof

Study-note section NET02

PAN connects personal devices, such as Bluetooth accessories. LAN covers a local building or campus; MAN spans a metropolitan region; WAN connects distant regions. Device count alone does not determine the category. The Internet is a global network of networks, commonly the largest example of a WAN.

Study-note section NET11

A firewall allows, rejects or inspects traffic under a security policy; it does not necessarily encrypt. A VPN, Virtual Private Network, provides a logical private connection over another network; a secure VPN authenticates/encrypts its tunnel. A modem modulates outgoing and demodulates incoming carrier signals. These functions may coexist in one home router but remain conceptually distinct.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 22 | lines 26-44

Personal Area Network (PAN): is a network may be spanned across a given table with distances between the devices not more than few meters. The technology used to interconnect the devices could be a Bluetooth. These networks are called Personal Area Networks, since the devices interconnected in these networks are belongs to a single person.
Local Area Network (LAN): is a network that may span across a building, or across several buildings within a single organization, by using intermediate devices, like switches and/or hubs, to interconnect devices in all floors.
Metropolitan Area Network (MAN): is a network that may span across a whole city interconnecting several buildings and organizations.
Wide Area Network (WAN): is a network that may span across multiple cities, or an entire country, or an entire continent or it may even cover the whole world. For example, an Internet is one example of WAN.

Question sources

Data Communication & Networking practice questions · Question 10

Question 107 | Q01531

A _____ is a device that forwards packets between networks by processing the routing information included in the packet.

A. bridge

B. firewall

C. router

D. hub

Hint

Compare signal repetition, frame forwarding, packet routing and policy enforcement using the stated device or traffic assumptions.

Answer C: router

Router forwarding explicitly compares the destination IP to routing table entries to choose the next path between networks. Evidence: PDF 12, 12, 12, 48.

Why each choice is right or wrong

A - Incorrect: Bridge filters same-protocol LAN traffic using MAC (PDF 12, 12, 12, 48.)

B - Incorrect: A firewall permits/denies access; that is not the defining routing-table function (PDF 12, 12, 12, 48.)

C - Correct: Router matches the stated destination-IP routing procedure (PDF 12, 12, 12, 48.)

D - Incorrect: Hub repeats/broadcasts without destination-route analysis (PDF 12, 12, 12, 48.)

Primary note proof

Study-note section NET11

> Routers forward IP packets between networks using destination prefixes and next hops. They separate broadcast domains and normally do not forward local link broadcasts. A default gateway is usually a router, while a protocol gateway can translate application formats; therefore a gateway is not inherently a device that implements every OSI layer.

Study-note section NET09

> A repeater regenerates layer-1 signals without inspecting destination addresses. An active hub is a multiport repeater: it repeats incoming signals onto other ports, placing half-duplex endpoints in one collision domain. A passive hub is a connector. A hub neither learns MAC addresses nor eliminates collisions. An endpoint such as a network printer consumes services; routers, hubs and access points are intermediary devices.

Study-note section NET10

> A bridge or ordinary Ethernet switch operates at layer 2. It learns source-MAC-to-port mappings, looks up the destination, forwards a known unicast to its port, filters it if the destination is on the incoming segment, and floods an unknown unicast or broadcast within its VLAN. A switch does

not always send only to one destination port. Wireless access points normally bridge wireless and wired link-layer traffic.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 12 | lines 38-52

ROUTER: Router is a specialized network device
used tointerconnect different types of network that
uses different protocol.
Router allows the users to connect several LAN and WAN
• A LAN to another LAN
• A WAN to another WAN
• A LAN to the Internet
Routers use the routing table to determine how to
forwardpackets.
• The list of routing tables provides directions to
transfer the data to a particular network
destination -various paths to forward the data.
• A router analyzes a destination IP address of a
givenpacket and compares it with the routing
table to decide the packet's next best path

Data Communication and Computer Networking module | PDF page 12 | lines 60-61

BRIDGE: Connects two LANS having the same protocol -
(e.g. Ethernet or Token ring).

Data Communication and Computer Networking module | PDF page 12 | lines 17-26

Active Hubs
An active hub is actually a multipart repeater. It is
normallyused to create connections between stations in
a physical startopology.
HUB: Hubs are commonly used to connect segments
(devices)of a LAN. Hubs don‘t filter information; instead
broadcast incoming packets to all computers connected to
it. A hub contains multiple ports which support 8, 12 or
24 RJ-45 ports. Two types: Passive hub and Active hub. It
is used in star or ring topology.

Data Communication and Computer Networking module | PDF page 48 | lines 29-40

Network Address Translation (NAT)
NAT translates the IP addresses of computers in a local
network to a single IP address. This address is often used
by the router that connects the computers to the Internet.
The router can be connected to a DSL modem, cable
modem, T1 line, or even a dial-up modem. When other
computers on the Internet attempt to access computers

within the local network, they only see the IP address of the router. This adds an extra level of security, since the router can be configured as a firewall, only allowing authorized systems to access the computers within the network.

Question sources

Data Communication & Networking practice questions · Question 11

Question 108 | Q01532

The physical layer is concerned with _____

A. bit-by-bit delivery

B. process to process delivery

C. application to application delivery

D. port to port delivery

Hint

Match the requested scope or data unit to the layer duties in the note; distinguish hop delivery from end-to-end process delivery.

Answer A: bit-by-bit delivery

Physical-layer standardized interfaces deliver bit-by-bit or symbol-by-symbol; processes and ports are transport concerns. Evidence: PDF 14, 16.

Why each choice is right or wrong

A - Correct: Bit-by-bit delivery is explicit (PDF 14, 16.)

B - Incorrect: Process delivery is transport (PDF 14, 16.)

C - Incorrect: Applications communicate through upper and transport services, not the physical bit interface (PDF 14, 16.)

D - Incorrect: Ports identify transport processes (PDF 14, 16.)

Primary note proof

Study-note section NET12

Sending proceeds from application data to transport segment/datagram, network packet, link frame and physical bits/symbols; receiving reverses the order. Each layer serves the layer above. A router removes a received link frame, inspects IP, and creates a new link frame for the next hop. MAC addresses usually change across routed hops; end-to-end IP addresses ordinarily remain until translation.

Study-note section NET17

Ports identify transport endpoints; the application can choose a transport and request socket buffer sizes, subject to OS limits. A TCP connection is identified by source/destination IP and source/destination port, with TCP understood. IPv4 protocol numbers identify upper protocols; 80 is a usual HTTP port, not an IP protocol number. Clients often use ephemeral ports. SCTP is a reliable message-oriented transport with multiple streams.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 14 | lines 32-49

Physical Layer:
• The Physical Layer provides a standardized interface to physical transmission media, including: Mechanical specification of electrical connectors and cables, for example maximum cable length, Electrical specification of transmission line and Bit-by-bit or symbol-by-symbol delivery.
• Interface: The Physical Layer defines the characteristics of interfaces between the devices & transmission medium.
• Representation of bits: The physical layer is concerned with transmission of signals from one device to another which involves converting data (1_s & 0_s) into signals and vice versa. It is not concerned with the meaning or interpretation of bits.
• Data rate: The physical layer defines the data transmission rate i.e. number of bits sent per second. It is the responsibility of the physical layer to maintain the defined data rate.

Data Communication and Computer Networking module | PDF page 16 | lines 2-17

• At the sending side, the transport layer receives data from the session layer, divides it into units called segments and sends it to the network layer.
• To ensure process to process delivery the transport layer makes use of port address to identify the data from the sending and receiving process.
• The data can be transported in a connection oriented or connectionless manner.
• The Transport layer is responsible for segmentation and reassembly of the message into segments which bear sequence numbers.
• The transport layer also carries out flow control and error control functions; but unlike data link layer these are end to end rather than node to node.
• The main responsibility of the transport layer is process to process delivery of the entire message

Question sources

Data Communication & Networking practice questions · Question 12

Question 109 | Q01533

A new network backbone needs high capacity, long reach and immunity to electromagnetic interference in the transmission medium. Which listed medium carries light rather than electrical signals and best matches these requirements?

A. coaxial cable

B. twisted pair cable

C. optical fiber

D. electrical cable

Hint

Compare the signal mechanism, medium properties or transmission direction against the definitions and stated physical assumptions.

Answer C: optical fiber

Optical fiber guides light, resists electromagnetic interference and supports high-capacity, long-reach links with suitable optics and installation. Twisted pair and coaxial cable carry electrical signals; their shielding or pair geometry can reduce interference but does not give the medium optical immunity. Exact speeds depend on the selected specification and equipment, so this comparison does not rank every possible fiber and copper product by speed.

Why each choice is right or wrong

A - Incorrect: Coaxial cable uses electrical signaling despite its shielding.

B - Incorrect: Twisted pair uses electrical signaling and reduces, rather than eliminates, coupled interference.

C - Correct: Optical fiber carries light and matches the stated capacity, reach and EMI requirements.

D - Incorrect: An electrical cable does not carry the required optical signal.

Primary note proof

Study-note section NET07

> Twisted pairs reduce coupled interference; UTP has no added shield and STP adds shielding. Coax has an inner conductor and outer shield sharing an axis. Fiber guides light and resists electromagnetic interference; it supports high capacity and long reach, but requires suitable optics and installation. Exact speed, cost and reach depend on the specification, not the material alone. Fiber can still be tapped.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 20 | lines 49-54

> Wavelength-division multiplexing (WDM): is designed to use the high-data-rate capability of fiber-optic cable. The optical fiber data rate is higher than the data rate of metallic transmission cable. Using a fiber-optic cable for one single line wastes the available bandwidth. Multiplexing allows us to combine several lines into one.

Data Communication and Computer Networking module | PDF page 11 | lines 23-33

> Twisted-pair cable: Consists of two conductors (normally copper), each with its own plastic insulation, twisted together.
> Two types
> • Unshielded Twisted-Pair cable (UTP)
> • Shielded Twisted-Pair cable (STP)
> Coaxial cable:- uses copper wire to conduct the signals electronically
> Fiber-optic cable:- uses glass or plastic conductor and transmits the signals as light
> Wireless/Unguided media the signal propagates in the atmosphere and in outer space

Question sources

Data Communication & Networking practice questions · Question 13

Question 110 | Q01534

Bits can be sent over guided and unguided media as analog signal by _____

A. digital modulation

B. amplitude modulation

C. frequency modulation

D. phase modulation

Hint

Compare the signal mechanism, medium properties or transmission direction against the definitions and stated physical assumptions.

Answer A: digital modulation

Digital modulation explicitly converts digital data to analog signals; ASK/FSK/PSK are its given methods. The other names are listed as analog modulation of analog data. Evidence: PDF 13.

Why each choice is right or wrong

A - Correct: Exactly the digital-to-analog conversion category (PDF 13.)

B - Incorrect: AM appears as analog modulation, not the digital-data category (PDF 13.)

C - Incorrect: FM appears as analog modulation, while digital frequency encoding is FSK (PDF 13.)

D - Incorrect: PM appears as analog modulation, while digital phase encoding is PSK (PDF 13.)

Primary note proof

Study-note section NET15

ASK varies carrier amplitude, FSK frequency, PSK phase; QAM combines amplitude and phase. AM/FM/PM can carry analog data. PCM digitizes analog input by sampling, quantizing and encoding. Sampling must exceed twice the highest retained baseband frequency in practical designs; b-bit samples have 2^b quantization levels and uncompressed rate fs×b. PAM/PWM are pulse modulation methods; pulse amplitude or width alone is not a binary PCM code.

Study-note section NET04

Analog signals vary continuously; digital signals use discrete symbol states. Data and signal types are separate: digital bits can modulate an analog carrier. A sine wave has amplitude, frequency and phase. Frequency f counts cycles/second, period T=1/f, and wavelength λ=v/f depends on propagation speed v. Phase specifies displacement within a cycle. Composite signals combine frequencies.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 13 | lines 65-77

• Digital modulation is used to convert digital data to
analog signal. Ex ASK, FSK, PSK.
Analog Modulation can be accomplished in three ways:
• Amplitude modulation (AM)
• Frequency modulation (FM)
• Phase modulation (PM).
Digital Modulation Types (Digital to Analog signal
conversion)
Digital modulation is used to convert digital data to analog
signal. It can be accomplished in the following ways:
• Amplitude Shift Keying(ASK)
• Frequency Shift keying (FSK)
• Phase Shift keying (PSK)

Question sources

Data Communication & Networking practice questions · Question 14

Question 111 | Q01535

The portion of physical layer that interfaces with the media access control sublayer is called _____

A. physical signalling sublayer

B. physical data sublayer

C. physical address sublayer

D. physical transport sublayer

Hint

Match the requested scope or data unit to the layer duties in the note; distinguish hop delivery from end-to-end process delivery.

Answer A: Physical Signaling (PLS) sublayer in legacy IEEE 802.3

NET09 gives the architecture-specific name Physical Signaling (PLS) for the PHY portion interfacing with MAC in legacy IEEE 802.3 AUI/MAU terminology. That directly matches A. The qualification matters because modern PHY descriptions can use other sublayers; this is not a universal OSI sublayer name. The other offered names do not match the defined legacy interface.

Why each choice is right or wrong

A - Correct: Physical Signaling, abbreviated PLS, is the MAC-facing sublayer identified for the legacy IEEE architecture.

B - Incorrect: Physical data sublayer is not the MAC-facing sublayer name defined in NET09.

C - Incorrect: Physical address concerns addressing terminology; it is not the stated legacy PHY interface sublayer.

D - Incorrect: Physical transport sublayer is not the architecture-specific PLS name established here.

Primary note proof

Study-note section NET09

> In the legacy IEEE 802.3 architecture with an attachment unit interface (AUI) and medium attachment unit (MAU), the MAC interfaces to the Physical Signaling (PLS) sublayer. For this legacy MAC interface, the relevant sublayer is PLS. This name is architecture-specific: other PHY designs use reconciliation (RS), physical coding (PCS), physical medium attachment (PMA) and related sublayers. Do not present PLS as a universal OSI sublayer name.

Study-note section NET09

> A NIC supplies a computer’s network interface and commonly implements both physical and link functions. Calling a NIC a physical interface does not mean all its functions are layer 1. Physical specifications include connectors, signaling, voltage, timing and physical coding/modulation; the PHY interface to MAC handles hardware signaling.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 14 | lines 32-49

Physical Layer:
• The Physical Layer provides a standardized interface to physical transmission media, including: Mechanical specification of electrical connectors and cables, for example maximum cable length, Electrical specification of transmission line and Bit-by-bit or symbol-by-symbol delivery.
• Interface: The Physical Layer defines the characteristics of interfaces between the devices & transmission medium.
• Representation of bits: The physical layer is concerned with transmission of signals from one device to another which involves converting data (1_s & 0_s) into signals and vice versa. It is not concerned with the meaning or interpretation of bits.
• Data rate: The physical layer defines the data transmission rate i.e. number of bits sent per second. It is the responsibility of the physical layer to maintain the defined data rate.

Data Communication and Computer Networking module | PDF page 15 | lines 13-40

Data Link Layer
• The Data Link layer adds reliability to the physical layer by providing error detection and correction mechanisms.
• Framing: the Data Link layer receives the data from Network Layer and divides the stream of bits into fixed size manageable units called as Frames and sends it to the physical layer. On the receiver side, the data link layer receives the stream of bits from the physical layer and regroups them into frames and sends them to the Network layer.
• Physical Addressing: The Data link layer appends the physical address in the header of the frame before sending it to physical layer.
• Flow control: The data link layer makes sure that the sender sends the data at a speed at which the receiver canreceive it else if there is an overflow at the receiver sidethe data will be lost.
• Error Control: The data link layer imposes error control mechanism to identify lost or damaged frames, duplicateframes and then retransmit them.
• Access Control: The data link layer imposes access control mechanism to determine which

device has right to send data in an multipoint connection setting.
• Main Responsibility: The main responsibility of the data link layer is hop to hop transmission of frames.

Question sources

Data Communication & Networking practice questions · Question 15

Question 112 | Q01536

Which option gives the most complete combined set of physical-layer specifications among those listed?

A. mechanical specifications of electrical connectors and cables

B. electrical specification of transmission line signal level

C. specification for IR over optical fiber

D. all of the mentioned

Hint

Match the requested scope or data unit to the layer duties in the note; distinguish hop delivery from end-to-end process delivery.

Answer D: All are physical-medium/signaling specifications

The physical layer specifies how signals and physical interfaces carry bits. Mechanical connector and cable requirements, electrical signal levels and optical signaling parameters all concern that role. Infrared signaling over suitable optical fiber is an optical physical-medium specification. Each individual item is therefore a valid example, but only the aggregate includes all three and satisfies the requested most-complete selection.

Why each choice is right or wrong

A - Incorrect: Mechanical connectors and cables are physical-layer specifications, but this alone omits the other valid items.

B - Incorrect: Electrical signal levels are physical-layer specifications, but this alone omits the other valid items.

C - Incorrect: Infrared optical signaling is a physical-medium specification, but this alone omits the other valid items.

D - Correct: All three items concern physical interfaces or signaling, so this is the complete combined response.

Primary note proof

Study-note section NET09

A NIC supplies a computer's network interface and commonly implements both physical and link functions. Calling a NIC a physical interface does not mean all its functions are layer 1. Physical specifications include connectors, signaling, voltage, timing and physical coding/modulation; the PHY interface to MAC handles hardware signaling.

Study-note section NET-S07

Fiber-optic links can use near-infrared light. The selected optical wavelength is part of the link's physical signaling specification, just as connectors and electrical signal levels are physical-interface specifications. This does not require every fiber link to use the same wavelength.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 14 | lines 32-49

Physical Layer:
• The Physical Layer provides a standardized interface to physical transmission media, including: Mechanical specification of electrical connectors and cables, for example maximum cable length, Electrical specification of transmission line and Bit-by-bit or symbol-by-symbol delivery.
• Interface: The Physical Layer defines the characteristics of interfaces between the devices & transmission medium.
• Representation of bits: The physical layer is concerned with transmission of signals from one device to another which involves converting data (1_s & 0_s) into signals and vice versa. It is not concerned with the meaning or interpretation of bits.
• Data rate: The physical layer defines the data transmission rate i.e. number of bits sent per second. It is the responsibility of the physical layer to maintain the defined data rate.

Data Communication and Computer Networking module | PDF page 11 | lines 23-33

Twisted-pair cable: Consists of two conductors (normally copper), each with its own plastic insulation, twisted together.
Two types
• Unshielded Twisted-Pair cable (UTP)
• Shielded Twisted-Pair cable (STP)
Coaxial cable:- uses copper wire to conduct the signals electronically
Fiber-optic cable:- uses glass or plastic conductor and transmits the signals as light
Wireless/Unguided media the signal propagates in the atmosphere and in outer space

Question sources

Data Communication & Networking practice questions · Question 16

Question 113 | Q01537

Which single option gives the complete set of listed operations that can be implemented as physical-layer transmission coding or modulation?

A. line coding

B. channel coding

C. modulation

D. all of the mentioned

Hint

Match the requested scope or data unit to the layer duties in the note; distinguish hop delivery from end-to-end process delivery.

Answer D: all of the mentioned

Physical transmission includes mapping bits to signal patterns and modulating carriers. Channel coding in this question means redundancy used in transmission coding, rather than every possible higher-layer error-control mechanism. Under that scope, all three operations can be physical-layer work. Each individual choice names only part of the qualifying set, so the inclusive option is the complete response.

Why each choice is right or wrong

A - Incorrect: Line coding is physical signaling work, but alone omits the other qualifying operations.

B - Incorrect: Physical channel coding adds transmission redundancy, but alone is incomplete.

C - Incorrect: Modulation is a physical transmission operation, but alone is incomplete.

D - Correct: Line coding, physical channel coding and modulation all qualify, making this the complete set.

Primary note proof

Study-note section NET09

> A NIC supplies a computer’s network interface and commonly implements both physical and link functions. Calling a NIC a physical interface does not mean all its functions are layer 1. Physical specifications include connectors, signaling, voltage, timing and physical coding/modulation; the PHY interface to MAC handles hardware signaling.

Study-note section NET15

> Line coding maps digital bits to digital signal patterns. NRZ uses levels without a forced mid-bit return; Manchester supplies a mid-bit transition for clocking, with bit convention specified. Differential Manchester encodes using transitions relative to previous state. AMI alternates the

polarity of successive ones; pseudoternary alternates zero pulses. Block coding adds code redundancy; scrambling replaces problematic patterns without necessarily increasing bit count. Multilevel schemes include 2B1Q and 8B6T; MLT-3 uses a sequence of voltage transitions.

Study-note section NET15

ASK varies carrier amplitude, FSK frequency, PSK phase; QAM combines amplitude and phase. AM/FM/PM can carry analog data. PCM digitizes analog input by sampling, quantizing and encoding. Sampling must exceed twice the highest retained baseband frequency in practical designs; b-bit samples have 2^b quantization levels and uncompressed rate fs×b. PAM/PWM are pulse modulation methods; pulse amplitude or width alone is not a binary PCM code.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 14 | lines 32-49

Physical Layer:
• The Physical Layer provides a standardized interface to physical transmission media, including: Mechanical specification of electrical connectors and cables, for example maximum cable length, Electrical specification of transmission line and Bit-by-bit or symbol-by-symbol delivery.
• Interface: The Physical Layer defines the characteristics of interfaces between the devices & transmission medium.
• Representation of bits: The physical layer is concerned with transmission of signals from one device to another which involves converting data (1_s & 0_s) into signals and vice versa. It is not concerned with the meaning or interpretation of bits.
• Data rate: The physical layer defines the data transmission rate i.e. number of bits sent per second. It is the responsibility of the physical layer to maintain the defined data rate.

Data Communication and Computer Networking module | PDF page 13 | lines 42-50

Digital Data to Digital Signal conversion
Coding methods are used to convert digital data into digital signals. There are two types of coding methods:
• Line Coding
• Block Coding
Scrambling is also one of the ways to convert digital data to digital signals but is not used.
Line Coding: It is the process of converting Digital data into digital signal.

Data Communication and Computer Networking module | PDF page 13 | lines 65-77

• Digital modulation is used to convert digital data to analog signal. Ex ASK, FSK, PSK.
Analog Modulation can be accomplished in three ways:
• Amplitude modulation (AM)
• Frequency modulation (FM)
• Phase modulation (PM).
Digital Modulation Types (Digital to Analog signal conversion)
Digital modulation is used to convert digital data to analog signal. It can be accomplished in the following ways:
• Amplitude Shift Keying(ASK)
• Frequency Shift keying (FSK)
• Phase Shift keying (PSK)

Data Communication and Computer Networking module | PDF page 13 | lines 27-37

Redundancy
In order to detect and correct the errors in the data communication we add some extra bits to the original data.
These extra bits are nothing but the redundant bits which will be removed by the receiver after receiving the data.
There are different techniques used for transmission error detection and correction.
Detection methods:
• Parity Check
• Cyclic Redundancy Check
• Checksum

Question sources

Data Communication & Networking practice questions · Question 17

Question 114 | Q01538

The physical layer translates logical communication requests from the _____ into hardware specific operations.

A. data link layer

B. network layer

C. trasnport layer

D. application layer

Hint

Match the requested scope or data unit to the layer duties in the note; distinguish hop delivery from end-to-end process delivery.

Answer A: data link layer

The module adjacent layer order places data link immediately above physical, and data link passes frames to physical for bit transmission. Evidence: PDF 14, 14, 15.

Why each choice is right or wrong

A - Correct: Data link directly supplies the physical layer (PDF 14, 14, 15.)

B - Incorrect: Network supplies data link first, not physical directly (PDF 14, 14, 15.)

C - Incorrect: Transport supplies network first (PDF 14, 14, 15.)

D - Incorrect: Application passes through several intervening layers (PDF 14, 14, 15.)

Primary note proof

Study-note section NET12

> Sending proceeds from application data to transport segment/datagram, network packet, link frame and physical bits/symbols; receiving reverses the order. Each layer serves the layer above. A router removes a received link frame, inspects IP, and creates a new link frame for the next hop. MAC addresses usually change across routed hops; end-to-end IP addresses ordinarily remain until translation.

Study-note section NET09

> A NIC supplies a computer's network interface and commonly implements both physical and link functions. Calling a NIC a physical interface does not mean all its functions are layer 1. Physical specifications include connectors, signaling, voltage, timing and physical coding/modulation; the PHY interface to MAC handles hardware signaling.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 14 | lines 12-29

> The Open Systems Interconnection (OSI) Model was
> developed by International Organization for Standardization
> (ISO). ISO is the organization, OSI is the model
> It was developed to allow systems with different platforms
> (Hardware & software) to communicate with each other.
> Now, it is a network model that defines the protocols for
> network communications.
> It is a hierarchical model that groups its processes into seven
> (7) layers. (Top to Bottom)
> 1. Application Layer
> 2. Presentation Layer
> 3. Session Layer
> 4. Transport Layer
> 5. Network Layer
> 6. Data Link Layer
> 7. Physical Layer

Each layer has specific functions to perform and has to co-operate with the layers above and below it.

Data Communication and Computer Networking module | PDF page 14 | lines 32-49

Physical Layer:
• The Physical Layer provides a standardized interface to physical transmission media, including: Mechanical specification of electrical connectors and cables, for example maximum cable length, Electrical specification of transmission line and Bit-by-bit or symbol-by-symbol delivery.
• Interface: The Physical Layer defines the characteristics of interfaces between the devices & transmission medium.
• Representation of bits: The physical layer is concerned with transmission of signals from one device to another which involves converting data (1_s & 0_s) into signals and vice versa. It is not concerned with the meaning or interpretation of bits.
• Data rate: The physical layer defines the data transmission rate i.e. number of bits sent per second. It is the responsibility of the physical layer to maintain the defined data rate.

Data Communication and Computer Networking module | PDF page 15 | lines 13-40

Data Link Layer
• The Data Link layer adds reliability to the physical layer by providing error detection and correction mechanisms.
• Framing: the Data Link layer receives the data from Network Layer and divides the stream of bits into fixed size manageable units called as Frames and sends it to the physical layer. On the receiver side, the data link layer receives the stream of bits from the physical layer and regroups them into frames and sends them to the Network layer.
• Physical Addressing: The Data link layer appends the physical address in the header of the frame before sending it to physical layer.
• Flow control: The data link layer makes sure that the sender sends the data at a speed at which the receiver canreceive it else if there is an overflow at the receiver sidethe data will be lost.
• Error Control: The data link layer imposes error control mechanism to identify lost or damaged frames, duplicateframes and then retransmit them.
• Access Control: The data link layer imposes

access control mechanism to determine which device has right to send data in an multipoint connection setting.
• Main Responsibility: The main responsibility of the data link layer is hop to hop transmission of frames.

Question sources

Data Communication & Networking practice questions · Question 18

Question 115 | Q01539

A single channel is shared by multiple signals by _____

A. analog modulation

B. digital modulation

C. multiplexing

D. phase modulation

Hint

Compare the signal mechanism, medium properties or transmission direction against the definitions and stated physical assumptions.

Answer C: multiplexing

The module defines multiplexing as simultaneous multiple signals across a single data link. Evidence: PDF 20, 13.

Why each choice is right or wrong

A - Incorrect: Analog modulation changes a carrier rather than defining shared-channel combination (PDF 20, 13.)

B - Incorrect: Digital modulation converts digital data to analog signals (PDF 20, 13.)

C - Correct: Multiplexing is the explicit shared-channel technique (PDF 20, 13.)

D - Incorrect: Phase modulation is one carrier parameter method (PDF 20, 13.)

Primary note proof

Study-note section NET32

Multiplexing combines multiple input streams onto a shared link; demultiplexing separates them at the receiver. It differs from broadcasting one message to many destinations. FDM assigns distinct frequency bands with suitable guard spacing; WDM assigns different optical wavelengths. TDM allocates time slots: synchronous TDM reserves recurrent slots even if an input is idle, while statistical TDM allocates according to demand and needs identification.

Study-note section NET15

ASK varies carrier amplitude, FSK frequency, PSK phase; QAM combines amplitude and phase. AM/FM/PM can carry analog data. PCM digitizes analog input by sampling, quantizing and encoding. Sampling must exceed twice the highest retained baseband frequency in practical designs; b-bit samples have 2^b quantization levels and uncompressed rate fs×b. PAM/PWM are pulse modulation methods; pulse amplitude or width alone is not a binary PCM code.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 20 | lines 37-42

MULTIPLEXING
Whenever the bandwidth of a medium linking two devices is greater than the bandwidth needs of the devices, the link can be shared. Multiplexing is the set of techniques that allows the simultaneous transmission of multiple signals across a single data link.

Data Communication and Computer Networking module | PDF page 13 | lines 65-77

• Digital modulation is used to convert digital data to analog signal. Ex ASK, FSK, PSK.
Analog Modulation can be accomplished in three ways:
• Amplitude modulation (AM)
• Frequency modulation (FM)
• Phase modulation (PM).
Digital Modulation Types (Digital to Analog signal conversion)
Digital modulation is used to convert digital data to analog signal. It can be accomplished in the following ways:
• Amplitude Shift Keying(ASK)
• Frequency Shift keying (FSK)
• Phase Shift keying (PSK)

Question sources

Data Communication & Networking practice questions · Question 19

Question 116 | Q01540

The data link layer takes the packets from _____ and encapsulates them into frames for transmission.

A. network layer

B. physical layer

C. transport layer

D. application layer

Hint

Match the requested scope or data unit to the layer duties in the note; distinguish hop delivery from end-to-end process delivery.

Answer A: network layer

The sending-side data link explicitly receives network-layer data and frames it for physical transmission. Evidence: PDF 15, 16, 15.

Why each choice is right or wrong

A - Correct: Network is the immediately preceding sender-side layer (PDF 15, 16, 15.)

B - Incorrect: Physical is the lower receive-side source of bits, not upper packets (PDF 15, 16, 15.)

C - Incorrect: Transport provides segments to network first (PDF 15, 16, 15.)

D - Incorrect: Application is several layers above framing (PDF 15, 16, 15.)

Primary note proof

Study-note section NET12

> Sending proceeds from application data to transport segment/datagram, network packet, link frame and physical bits/symbols; receiving reverses the order. Each layer serves the layer above. A router removes a received link frame, inspects IP, and creates a new link frame for the next hop. MAC addresses usually change across routed hops; end-to-end IP addresses ordinarily remain until translation.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 15 | lines 13-40

> Data Link Layer
> • The Data Link layer adds reliability to the physical layer by providing error detection and correction mechanisms.
> • Framing: the Data Link layer receives the data from Network Layer and divides the stream of bits into fixed size manageable units called as Frames and sends it to the physical layer. On the receiver side, the data link layer receives the stream of bits from the physical layer and regroups them into frames and sends them to the Network layer.
> • Physical Addressing: The Data link layer appends the physical address in the header of the frame before sending it to physical layer.
> • Flow control: The data link layer makes sure that the sender sends the data at a speed at which the receiver canreceive it else if there is an overflow at the receiver sidethe data will be lost.

• Error Control: The data link layer imposes error control mechanism to identify lost or damaged frames, duplicateframes and then retransmit them.
• Access Control: The data link layer imposes access control mechanism to determine which device has right to send data in an multipoint connection setting.
• Main Responsibility: The main responsibility of the data link layer is hop to hop transmission of frames.

Data Communication and Computer Networking module | PDF page 16 | lines 2-17

• At the sending side, the transport layer receives data from the session layer, divides it into units called segments and sends it to the network layer.
• To ensure process to process delivery the transport layer makes use of port address to identify the data from the sending and receiving process.
• The data can be transported in a connection oriented or connectionless manner.
• The Transport layer is responsible for segmentation and reassembly of the message into segments which bear sequence numbers.
• The transport layer also carries out flow control and error control functions; but unlike data link layer these are end to end rather than node to node.
• The main responsibility of the transport layer is process to process delivery of the entire message

Data Communication and Computer Networking module | PDF page 15 | lines 41-61

Network Layer
• The network layer makes sure that the data is deliveredto the receiver despite multiple intermediate devices.
• The network layer at the sending side accepts data from the transport layer, divides it into packets, addsaddressing information in the header and passes it tothe data link layer.
• The network layer is responsible for source todestination of delivery of data.
• The network layer uses logical address commonlyknown as IP address to recognize devices on the network.
• Each packet is independent of the other and may travelusing different routes to reach the receiver hence may arrive out of turn at the receiver

(Routing).
• The Network layer does not perform any flow controlor error control
• The main responsibility of Network Layer is transmission of packets from source to destination

Question sources

Data Communication & Networking practice questions · Question 20

Question 117 | Q01541

Wireless transmission of signals can be done via _____

A. radio waves

B. microwaves

C. infrared

D. all of the mentioned

Hint

Compare the signal mechanism, medium properties or transmission direction against the definitions and stated physical assumptions.

Answer D: all of the mentioned

The module explicitly lists radio waves, microwaves and infrared as three unguided wireless media. Evidence: PDF 10.

Why each choice is right or wrong

A - Incorrect: Radio waves are listed (PDF 10.)

B - Incorrect: Microwaves are listed (PDF 10.)

C - Incorrect: Infrared is listed (PDF 10.)

D - Correct: All three appear in the unguided-media list (PDF 10.)

Primary note proof

Study-note section NET07

Radio, microwave and infrared are unguided media. Ground waves follow Earth, sky waves can reflect from ionized layers, and line-of-sight paths require suitable visibility. Microwaves are radio waves in the broader physical classification. Infrared generally does not penetrate walls. Directionality depends on antennas: omnidirectional means broad azimuth coverage, not equal radiation in every 3-D direction. Legacy Ethernet straight-through cables join unlike MDI/MDI-X roles; crossover joins like roles, such as PC-PC or switch-switch. Auto-MDI-X can remove that requirement.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 10 | lines 36-55

TRANSMISSION MEDIA
Transmission media is a means by which a communicationsignal is carried from one system to another
A transmission medium can be defined as anything that cancarry information from a source to a destination. The transmission medium is usually free space, metallic cable orfiber optic cable. Guided and Unguided (WIRELESS) Guided Transmission Media uses a cabling system that guidesthe data signals along a specific path. Out of these twisted-paircable, coaxial cable transport signals in the form of electricsignals and fiber-optic cable transport signals in the form oflight. Unguided Transmission Media transport data without using a physical conductor. It uses wireless electromagnetic signals to send data. Three types of unguided media:
• Radio waves
• Micro waves
• Infrared.

Question sources

Data Communication & Networking practice questions · Question 21

Question 118 | Q01542

Under the OSI role convention used here, which task belongs to physical transmission coding rather than data-link framing and control? Here channel coding means physical-channel coding, not a link-frame CRC or retransmission procedure.

A. framing

B. error control

C. flow control

D. channel coding

Hint

Match the requested scope or data unit to the layer duties in the note; distinguish hop delivery from end-to-end process delivery.

Answer D: channel coding

The data-link layer packages data into frames and can provide hop-local error and flow control. Physical transmission coding concerns how the channel carries the signal and any coding assigned to that physical role. The explicit convention distinguishes physical-channel coding from link error-detection redundancy or ARQ; without that scope, the broad term coding could overlap link functions.

Why each choice is right or wrong

A - Incorrect: Framing packages hop-delivery data into link frames.

B - Incorrect: Link error control includes detection and protocol-dependent recovery.

C - Incorrect: Link flow control regulates hop-local sending when supported.

D - Correct: Physical-channel coding is outside the stated link framing/control role.

Primary note proof

Study-note section NET13

> Link-layer LLC identifies or multiplexes upper-layer protocols and may supply link control; MAC handles medium-dependent addressing/access and frame delivery. Network addressing belongs to layer 3. Ethernet, PPP and HDLC are link protocols. Frame headers may carry addresses and control/type fields; synchronization and exact framing depend on the protocol.

Study-note section NET14

> Controlled access uses polling, reservations or a token to grant turns; correctly coordinated access avoids contention collisions. Channelization divides frequency, time or code resources. Stop-and-wait sends one frame and waits for ACK, retransmitting on timeout; sequence bits distinguish duplicates. Sliding windows permit multiple unacknowledged frames. Link reliability/flow control is hop-local; transport reliability/flow control is end-to-end. Ethernet detects corruption but does not itself guarantee reliable delivery.

Study-note section NET09

> A NIC supplies a computer’s network interface and commonly implements both physical and link functions. Calling a NIC a physical interface does not mean all its functions are layer 1. Physical specifications include connectors, signaling, voltage, timing and physical coding/modulation; the PHY interface to MAC handles hardware signaling.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 15 | lines 13-40

> Data Link Layer
> • The Data Link layer adds reliability to the physical layer by providing error detection and correction mechanisms.
> • Framing: the Data Link layer receives the data from Network Layer and divides the stream of bits

into fixed size manageable units called as Frames and sends it to the physical layer. On the receiver side, the data link layer receives the stream of bits from the physical layer and regroups them into frames and sends them to the Network layer.
• Physical Addressing: The Data link layer appends the physical address in the header of the frame before sending it to physical layer.
• Flow control: The data link layer makes sure that the sender sends the data at a speed at which the receiver canreceive it else if there is an overflow at the receiver sidethe data will be lost.
• Error Control: The data link layer imposes error control mechanism to identify lost or damaged frames, duplicateframes and then retransmit them.
• Access Control: The data link layer imposes access control mechanism to determine which device has right to send data in an multipoint connection setting.
• Main Responsibility: The main responsibility of the data link layer is hop to hop transmission of frames.

Data Communication and Computer Networking module | PDF page 13 | lines 42-50

Digital Data to Digital Signal conversion
Coding methods are used to convert digital data into digital signals. There are two types of coding methods:
• Line Coding
• Block Coding
Scrambling is also one of the ways to convert digital data to digital signals but is not used.
Line Coding: It is the process of converting Digital data into digital signal.

Data Communication and Computer Networking module | PDF page 13 | lines 27-37

Redundancy
In order to detect and correct the errors in the data communication we add some extra bits to the original data. These extra bits are nothing but the redundant bits which will be removed by the receiver after receiving the data.
There are different techniques used for transmission error detection and correction.
Detection methods:
• Parity Check
• Cyclic Redundancy Check
• Checksum

Question sources

Data Communication & Networking practice questions · Question 22

Question 119 | Q01543

Which sublayer of the data link layer performs data link functions that depend upon the type of medium?

A. logical link control sublayer

B. media access control sublayer

C. network interface control sublayer

D. error control sublayer

Hint

Match the requested scope or data unit to the layer duties in the note; distinguish hop delivery from end-to-end process delivery.

Answer B: Media Access Control (MAC)

The decisive phrase is “depend upon the type of medium.” NET13 assigns medium-dependent addressing, access and frame delivery to MAC. LLC instead identifies or multiplexes upper-layer protocols. The other names do not designate the LLC/MAC subdivision established in the note, so they cannot replace the specific MAC role.

Why each choice is right or wrong

A - Incorrect: LLC identifies upper-layer protocols and supplies link control rather than the medium-dependent access role.

B - Correct: MAC performs the medium-dependent addressing and access functions explicitly named in NET13.

C - Incorrect: A network interface is hardware/functionality, not the named medium-dependent data-link sublayer in this division.

D - Incorrect: Error control is a function; it is not the LLC/MAC sublayer name for medium-dependent access.

Primary note proof

Study-note section NET13

> Link-layer LLC identifies or multiplexes upper-layer protocols and may supply link control; MAC handles medium-dependent addressing/access and frame delivery. Network addressing belongs to layer 3. Ethernet, PPP and HDLC are link protocols. Frame headers may carry addresses and control/type fields; synchronization and exact framing depend on the protocol.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 15 | lines 13-40

Data Link Layer
• The Data Link layer adds reliability to the physical layer by providing error detection and correction mechanisms.
• Framing: the Data Link layer receives the data from Network Layer and divides the stream of bits into fixed size manageable units called as Frames and sends it to the physical layer. On the receiver side, the data link layer receives the stream of bits from the physical layer and regroups them into frames and sends them to the Network layer.
• Physical Addressing: The Data link layer appends the physical address in the header of the frame before sending it to physical layer.
• Flow control: The data link layer makes sure that the sender sends the data at a speed at which the receiver canreceive it else if there is an overflow at the receiver sidethe data will be lost.
• Error Control: The data link layer imposes error control mechanism to identify lost or damaged frames, duplicateframes and then retransmit them.
• Access Control: The data link layer imposes access control mechanism to determine which device has right to send data in an multipoint connection setting.
• Main Responsibility: The main responsibility of the data link layer is hop to hop transmission of frames.

Data Communication and Computer Networking module | PDF page 21 | lines 6-26

MEDIUM ACCESS CONTROL
The problem of controlling the access to the medium is similarto the rules of speaking in a meeting (the right to speak isupheld; two people do not speak at the same time; do notinterrupt each other; do not monopolize the discussion; ...) Three categories of multiple access protocols
Random Access Protocols - try your best like taxis do
• MA - Multiple Access
• CSMA - Carrier Sense MA
• CSMA/CD - CSMA with Collision Detection
• CSMA/CA - CSMA with Collision AvoidanceControlled-Access Protocols - get permission
• Reservation
• Polling

• Token Passing
Channelization Protocols - simultaneous use
• FDMA - Frequency-Division MA
• TDMA - Time-Division MA
• CDMA - Code-Division MA

Question sources

Data Communication & Networking practice questions · Question 23

Question 120 | Q01544

Which listed field identifies source or destination endpoints in a link-frame header, rather than synchronization or frame/control identification? Select one.

A. synchronization bytes

B. addresses

C. frame identifier

D. all of the mentioned

Hint

Use the cited note definitions to identify the requested function or scope, then check each alternative against that same rule.

Answer B: addresses

Address fields identify the source or destination endpoints associated with a frame. Synchronization information helps delimit or align reception, while a frame identifier or control field distinguishes a frame or its function. The question asks specifically for endpoint identification, so the address option is the complete answer. Exact field placement depends on the link protocol and is not assumed universal.

Why each choice is right or wrong

A - Incorrect: Synchronization concerns alignment or boundaries rather than endpoint identity.

B - Correct: Address fields identify frame endpoints, matching the requested role.

C - Incorrect: A frame identifier distinguishes a frame or control function rather than its endpoint addresses.

D - Incorrect: The other listed fields have different roles, so all is not the endpoint-identification answer.

Primary note proof

Study-note section NET13

Link-layer LLC identifies or multiplexes upper-layer protocols and may supply link control; MAC handles medium-dependent addressing/access and frame delivery. Network addressing belongs

to layer 3. Ethernet, PPP and HDLC are link protocols. Frame headers may carry addresses and control/type fields; synchronization and exact framing depend on the protocol.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 15 | lines 13-40

Data Link Layer
• The Data Link layer adds reliability to the physical layer by providing error detection and correction mechanisms.
• Framing: the Data Link layer receives the data from Network Layer and divides the stream of bits into fixed size manageable units called as Frames and sends it to the physical layer. On the receiver side, the data link layer receives the stream of bits from the physical layer and regroups them into frames and sends them to the Network layer.
• Physical Addressing: The Data link layer appends the physical address in the header of the frame before sending it to physical layer.
• Flow control: The data link layer makes sure that the sender sends the data at a speed at which the receiver canreceive it else if there is an overflow at the receiver sidethe data will be lost.
• Error Control: The data link layer imposes error control mechanism to identify lost or damaged frames, duplicateframes and then retransmit them.
• Access Control: The data link layer imposes access control mechanism to determine which device has right to send data in an multipoint connection setting.
• Main Responsibility: The main responsibility of the data link layer is hop to hop transmission of frames.

Data Communication and Computer Networking module | PDF page 26 | lines 14-28

medium. TCP/IP was designed to be independent of the network access method, frame format, and medium. In this way, TCP/IP can be used to connect differing network types. These include LAN technologies such as Ethernet and Token Ring and WAN technologies such as X.25 and Frame Relay. Independence from any specific network technology gives TCP/IP the ability to be adapted to new technologies such as Asynchronous Transfer Mode (ATM).

Network Access layer uses a physical address to identify hosts and to deliver data.
The Network Access layer PDU is called a frame. It contains the IP packet as well as a protocol header and trailer from this layer.

Question sources

Data Communication & Networking practice questions · Question 24

Question 121 | Q01545

CRC stands for _____

A. cyclic redundancy check

B. code repeat check

C. code redundancy check

D. cyclic repeat check

Hint

Find the full expansion in the terminology note and compare each word rather than only matching initials.

Answer A: cyclic redundancy check

The error-detection list explicitly spells out Cyclic Redundancy Check, matching CRC initials. Evidence: PDF 13.

Why each choice is right or wrong

A - Correct: Cyclic Redundancy Check is the exact listed phrase (PDF 13.)

B - Incorrect: Code repeat check is not the expansion listed (PDF 13.)

C - Incorrect: Code redundancy check changes Cyclic to Code (PDF 13.)

D - Incorrect: Cyclic repeat check changes Redundancy to repeat (PDF 13.)

Primary note proof

Study-note section NET-S04

CRC expands to Cyclic Redundancy Check.

Study-note section NET13

Detection adds redundancy but does not guarantee correction. Even parity adds a bit so the total number of ones is even: 1011 needs parity 1. It detects every odd number of bit flips but misses even counts. CRC treats bits as a polynomial and appends the XOR-division remainder; the receiver repeats the division. Internet checksums add words with end-around carry and complement the sum. A burst spans from the first corrupted bit through the last, including

unchanged interior bits. Retransmission or sufficient forward-error-correcting redundancy is needed for recovery.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 13 | lines 27-37

Redundancy
In order to detect and correct the errors in the data communication we add some extra bits to the original data. These extra bits are nothing but the redundant bits which will be removed by the receiver after receiving the data.
There are different techniques used for transmission error detection and correction.
Detection methods:
• Parity Check
• Cyclic Redundancy Check
• Checksum

Question sources

Data Communication & Networking practice questions · Question 25

Question 122 | Q01546

Which single option gives the complete set of listed data-link protocols?

A. ethernet

B. point to point protocol

C. hdlc

D. all of the mentioned

Hint

Identify the requested service or delivery guarantee, then distinguish application roles, transport behavior and address configuration.

Answer D: all of the mentioned

Ethernet, PPP and HDLC are all link protocols. The question asks for the complete set among the listed choices, so selecting any one protocol alone omits two other valid members. The inclusive response therefore supplies the complete answer. This classification concerns the data-link protocol role and does not deny that a technology such as Ethernet also specifies physical signaling.

Why each choice is right or wrong

A - Incorrect: ethernet is a link protocol, but this option alone omits the other qualifying protocols.

B - Incorrect: point to point protocol is a link protocol, but this option alone omits the other qualifying protocols.

C - Incorrect: hdlc is a link protocol, but this option alone omits the other qualifying protocols.

D - Correct: Ethernet, PPP and HDLC all qualify; the combined option gives the complete set.

Primary note proof

Study-note section NET13

> Link-layer LLC identifies or multiplexes upper-layer protocols and may supply link control; MAC handles medium-dependent addressing/access and frame delivery. Network addressing belongs to layer 3. Ethernet, PPP and HDLC are link protocols. Frame headers may carry addresses and control/type fields; synchronization and exact framing depend on the protocol.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 26 | lines 14-28

> medium. TCP/IP was designed to be independent
> of the network access method, frame format, and
> medium. In this way, TCP/IP can be used to
> connect differing network types. These include
> LAN technologies such as Ethernet and Token
> Ring and WAN technologies such as X.25 and
> Frame Relay. Independence from any specific
> network technology gives TCP/IP the ability to
> be adapted to new technologies such as
> Asynchronous Transfer Mode (ATM).
> Network Access layer uses a physical address to
> identify hosts and to deliver data.
> The Network Access layer PDU is called a frame.
> It contains the IP packet as well as a protocol
> header and trailer from this layer.

Data Communication and Computer Networking module | PDF page 15 | lines 13-40

> Data Link Layer
> • The Data Link layer adds reliability to the physical
> layer by providing error detection and correction
> mechanisms.
> • Framing: the Data Link layer receives the data
> from Network Layer and divides the stream of bits
> into fixed size manageable units called as Frames
> and sends it to the physical layer. On the receiver
> side, the data link layer receives the stream of bits
> from the physical layer and regroups them into
> frames and sends them to the Network layer.
> • Physical Addressing: The Data link layer appends
> the physical address in the header of the frame

before sending it to physical layer.
• Flow control: The data link layer makes sure that the sender sends the data at a speed at which the receiver canreceive it else if there is an overflow at the receiver sidethe data will be lost.
• Error Control: The data link layer imposes error control mechanism to identify lost or damaged frames, duplicateframes and then retransmit them.
• Access Control: The data link layer imposes access control mechanism to determine which device has right to send data in an multipoint connection setting.
• Main Responsibility: The main responsibility of the data link layer is hop to hop transmission of frames.

Question sources

Data Communication & Networking practice questions · Question 26

Question 123 | Q01547

Which option gives the complete set of listed CSMA multiple-access mechanisms for shared-channel contention?

A. CSMA/CD

B. CSMA/CA

C. Both CSMA/CD & CSMA/CA

D. HDLC

Hint

Identify the requested service or delivery guarantee, then distinguish application roles, transport behavior and address configuration.

Answer C: Both CSMA/CD & CSMA/CA

CSMA/CD and CSMA/CA both govern shared-medium access. Legacy half-duplex Ethernet uses collision detection and backoff, while Wi-Fi uses collision avoidance procedures with waiting, backoff and acknowledgments. Selecting only one omits another valid listed mechanism. HDLC is a link framing/control protocol rather than either of these CSMA contention mechanisms, so the combined CSMA option is complete.

Why each choice is right or wrong

A - Incorrect: CSMA/CD is a valid mechanism but omits the other listed CSMA mechanism.

B - Incorrect: CSMA/CA is a valid mechanism but omits the other listed CSMA mechanism.

C - Correct: This includes both listed CSMA contention mechanisms.

D - Incorrect: HDLC is a link framing/control protocol, not a listed CSMA medium-contention mechanism.

Primary note proof

Study-note section NET14

> Random access allows contention: ALOHA sends opportunistically; CSMA senses before sending. In legacy half-duplex Ethernet, CSMA/CD detects collision, sends a jam indication, stops, and retries after random backoff. The jam signals a collision, not its clearance. Wi-Fi 802.11 uses CSMA/CA with waiting/backoff and acknowledgments; sensing does not eliminate hidden-terminal collisions.

Study-note section NET14

> Controlled access uses polling, reservations or a token to grant turns; correctly coordinated access avoids contention collisions. Channelization divides frequency, time or code resources. Stop-and-wait sends one frame and waits for ACK, retransmitting on timeout; sequence bits distinguish duplicates. Sliding windows permit multiple unacknowledged frames. Link reliability/flow control is hop-local; transport reliability/flow control is end-to-end. Ethernet detects corruption but does not itself guarantee reliable delivery.

Study-note section NET13

> Link-layer LLC identifies or multiplexes upper-layer protocols and may supply link control; MAC handles medium-dependent addressing/access and frame delivery. Network addressing belongs to layer 3. Ethernet, PPP and HDLC are link protocols. Frame headers may carry addresses and control/type fields; synchronization and exact framing depend on the protocol.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 21 | lines 6-26

> MEDIUM ACCESS CONTROL
> The problem of controlling the access to the medium is similarto the rules of speaking in a meeting (the right to speak isupheld; two people do not speak at the same time; do notinterrupt each other; do not monopolize the discussion; ...) Three categories of multiple access protocols
> Random Access Protocols - try your best like taxis do
> • MA - Multiple Access
> • CSMA - Carrier Sense MA
> • CSMA/CD - CSMA with Collision Detection
> • CSMA/CA - CSMA with Collision AvoidanceControlled-Access Protocols - get permission
> • Reservation
> • Polling

• Token Passing
Channelization Protocols - simultaneous use
• FDMA - Frequency-Division MA
• TDMA - Time-Division MA
• CDMA - Code-Division MA

Question sources

Data Communication & Networking practice questions · Question 27

Question 124 | Q01548

The network layer is concerned with _____ of dat
a.

A. bits

B. frames

C. packets

D. bytes

Hint

Match the requested scope or data unit to the layer duties in the note; distinguish hop delivery from end-to-end process delivery.

Answer C: packets

Despite the broken dat/a line ending, the identifiable concept is the network-layer unit: packets. Evidence: PDF 15, 15, 16, 14.

Why each choice is right or wrong

A - Incorrect: Bits are physical units (PDF 15, 15, 16, 14.)

B - Incorrect: Frames are data-link units (PDF 15, 15, 16, 14.)

C - Correct: Packets are explicitly formed and transmitted by network layer (PDF 15, 15, 16, 14.)

D - Incorrect: Bytes are not the named network PDU (PDF 15, 15, 16, 14.)

Primary note proof

Study-note section NET12

Sending proceeds from application data to transport segment/datagram, network packet, link frame and physical bits/symbols; receiving reverses the order. Each layer serves the layer above. A router removes a received link frame, inspects IP, and creates a new link frame for the next hop. MAC addresses usually change across routed hops; end-to-end IP addresses ordinarily remain until translation.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 15 | lines 41-61

Network Layer
• The network layer makes sure that the data is deliveredto the receiver despite multiple intermediate devices.
• The network layer at the sending side accepts data from the transport layer, divides it into packets, addsaddressing information in the header and passes it tothe data link layer.
• The network layer is responsible for source todestination of delivery of data.
• The network layer uses logical address commonlyknown as IP address to recognize devices on the network.
• Each packet is independent of the other and may travelusing different routes to reach the receiver hence may arrive out of turn at the receiver (Routing).
• The Network layer does not perform any flow controlor error control
• The main responsibility of Network Layer is transmission of packets from source to destination

Data Communication and Computer Networking module | PDF page 15 | lines 13-40

Data Link Layer
• The Data Link layer adds reliability to the physical layer by providing error detection and correction mechanisms.
• Framing: the Data Link layer receives the data from Network Layer and divides the stream of bits into fixed size manageable units called as Frames and sends it to the physical layer. On the receiver side, the data link layer receives the stream of bits from the physical layer and regroups them into frames and sends them to the Network layer.
• Physical Addressing: The Data link layer appends the physical address in the header of the frame before sending it to physical layer.
• Flow control: The data link layer makes sure that the sender sends the data at a speed at which the receiver canreceive it else if there is an overflow at the receiver sidethe data will be lost.
• Error Control: The data link layer imposes error control mechanism to identify lost or damaged

frames, duplicateframes and then retransmit them.
• Access Control: The data link layer imposes access control mechanism to determine which device has right to send data in an multipoint connection setting.
• Main Responsibility: The main responsibility of the data link layer is hop to hop transmission of frames.

Data Communication and Computer Networking module | PDF page 16 | lines 2-17

• At the sending side, the transport layer receives data from the session layer, divides it into units called segments and sends it to the network layer.
• To ensure process to process delivery the transport layer makes use of port address to identify the data from the sending and receiving process.
• The data can be transported in a connection oriented or connectionless manner.
• The Transport layer is responsible for segmentation and reassembly of the message into segments which bear sequence numbers.
• The transport layer also carries out flow control and error control functions; but unlike data link layer these are end to end rather than node to node.
• The main responsibility of the transport layer is process to process delivery of the entire message

Data Communication and Computer Networking module | PDF page 14 | lines 32-49

Physical Layer:
• The Physical Layer provides a standardized interface to physical transmission media, including: Mechanical specification of electrical connectors and cables, for example maximum cable length, Electrical specification of transmission line and Bit-by-bit or symbol-by-symbol delivery.
• Interface: The Physical Layer defines the characteristics of interfaces between the devices & transmission medium.
• Representation of bits: The physical layer is concerned with transmission of signals from one device to another which involves converting data (1_s & 0_s) into signals and vice versa. It is not concerned with the meaning or interpretation of bits.
• Data rate: The physical layer defines the data transmission rate i.e. number of bits sent per second. It is the responsibility of the physical layer to maintain the defined data rate.

Question sources

Data Communication & Networking practice questions · Question 28

Question 125 | Q01549

For IPv4 as described in the note, which listed function is not provided by IP itself? Here “error control” means header checksum error detection.

A. routing

B. inter-networking

C. congestion control

D. error control

Hint

Separate address width, syntax, reserved scope and the supplied prefix or historical classful convention.

Answer C: congestion control

IPv4 supports logical packet delivery across networks, including routing, and checks its header with a checksum. The use of error control therefore refers to detection, not reliable end-to-end recovery. TCP supplies congestion control to protect network capacity; IPv4 itself does not provide TCP’s congestion-control service. The question separates those protocol services instead of denying that the network layer ever detects errors.

Why each choice is right or wrong

A - Incorrect: Routing is explicitly a network-layer function, so it cannot be the requested exception.

B - Incorrect: Forwarding packets between networks is an established network-layer responsibility.

C - Correct: Congestion control of the kind protecting network capacity is a TCP service rather than a service supplied by IPv4 itself.

D - Incorrect: IPv4 detects header corruption with its checksum, so error detection is present under the stated meaning.

Primary note proof

Study-note section NET16

> The IPv4 checksum protects its header; IP does not lack error checking altogether. Identification, flags and offset support fragmentation. IPv4 sources and routers may fragment when allowed; reassembly occurs at the destination. If DF is set and the next MTU is too small, forwarding fails and an ICMP diagnostic may be returned.

Study-note section NET17

TCP offers a reliable ordered byte stream using sequence numbers, acknowledgments, retransmission and windows. Flow control protects the receiver; congestion control protects network capacity. UDP sends independent datagrams with ports and a checksum but no built-in setup, delivery guarantee, retransmission or ordering. Live interactive traffic may choose UDP when late data is less useful than lost data. Application protocols can add reliability over UDP.

Study-note section NET30

Routing computes paths; forwarding chooses a next hop for an individual packet. Select the matching route with the longest prefix, then apply the routing system's tie-breaking criteria. A default /0 matches when nothing more specific does. Static routes are configured; dynamic protocols exchange reachability. Distance vector uses neighbor estimates, while link state distributes link information and computes shortest paths. Interior protocols operate within an autonomous system; BGP exchanges routes between systems.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 15 | lines 41-61

Network Layer
• The network layer makes sure that the data is deliveredto the receiver despite multiple intermediate devices.
• The network layer at the sending side accepts data from the transport layer, divides it into packets, addsaddressing information in the header and passes it tothe data link layer.
• The network layer is responsible for source todestination of delivery of data.
• The network layer uses logical address commonlyknown as IP address to recognize devices on the network.
• Each packet is independent of the other and may travelusing different routes to reach the receiver hence may arrive out of turn at the receiver (Routing).
• The Network layer does not perform any flow controlor error control
• The main responsibility of Network Layer is transmission of packets from source to destination

Data Communication and Computer Networking module | PDF page 27 | lines 5-31

Internet Control Message Protocol (ICMP):
works at the Network layer and is used by IP for many different services. ICMP is a management protocol and messagingservice provider for IP. The following are some common events and messages that ICMP relates to:

Destination Unreachable: If a router can‘t send an IP datagram any further, it uses ICMP to send a message back to the sender, advising it of the situation.
Buffer Full: If a router‘s memory buffer for receiving incoming datagrams is full, it will use ICMP to send out this message until the congestion abates.
Hops: Each IP datagram is allotted a certain number of routers, called hops, to pass through. If it reaches its limitof hops before arriving at its destination, the last router to receive that datagram deletes it. The executioner router then uses ICMP to send an obituary message, informing the sending machine of the demise of its datagram.
Ping (Packet Internet Groper) uses ICMP echo messages to check the physical and logical connectivity of machineson a network.
Traceroute Using ICMP timeouts, Traceroute is used to discover the path a packet takes as it traverses an Internetwork.

Question sources

Data Communication & Networking practice questions · Question 29

Question 126 | Q01550

A 4 byte IP address consists of _____

A. only network address

B. only host address

C. network address & host address

D. network address & MAC address

Hint

Separate address width, syntax, reserved scope and the supplied prefix or historical classful convention.

Answer C: network address & host address

The module says an IP address encodes network and host numbers; physical/MAC addresses are separate. Evidence: PDF 18, 19, 17.

Why each choice is right or wrong

A - Incorrect: Only network omits the stated host part (PDF 18, 19, 17.)

B - Incorrect: Only host omits the stated network part (PDF 18, 19, 17.)

C - Correct: Network plus host matches the stated composition (PDF 18, 19, 17.)

D - Incorrect: MAC is a separate physical address, not part of the IP field (PDF 18, 19, 17.)

Primary note proof

Study-note section NET-S06

An IP address identifies a network interface rather than limiting a whole computer to one address. A computer or router can have several interfaces and addresses. Under a supplied IPv4 prefix, leading bits identify the network and the remaining bits identify an address within that network; a MAC address is a separate link-layer identifier.

Study-note section NET22

Write IPv4 as four decimal octets 0-255, or as 32 binary bits. Use weights 128,64,32,16,8,4,2,1 within each octet. Thus 11000001 10000011 00011011 11111111 is 193.131.27.255. A value such as 257 is impossible. Syntactic validity differs from assignability: an address ending .0 or .255 can be a host under some prefixes.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 18 | lines 45-54

IP addresses: IP address uniquely identifies a device on the
Internet. Every host and router on the Internet has an IP address,
which encodes its network number and host number.
• The combination is unique: in principle, no two
machines on the Internet have the same IP address.
• An IPv4 address is 32 bits long
• They are used in the Source address and Destination
address fields of IP packets.
• An IP address does not refer to a host but it refers to a
network interface.

Data Communication and Computer Networking module | PDF page 19 | lines 23-36

Classful addressing : In classful addressing, the
addressspace is divided into five classes: A, B, C,
D, and E.
• Netid and Hostid In classful addressing, an IP
addressin class A, B, or C is divided into netid
and hostid.
Subnetting: It allows a network to be split into several
parts for internal use but still act like a single network to
the outsideworld.
• To implement subnetting, the router needs a
subnet mask that indicates the split between
network + subnet number and host. Ex.

255.255.252.0/22. A‖/22‖ to indicate that the subnet mask is 22 bits long.

Data Communication and Computer Networking module | PDF page 17 | lines 44-53

ARP - Address Resolution Protocol: It is used to resolve thephysical address of a device on a network, where its logical address is known.
Physical address is the 48 bit address that is imprinted on theNIC or LAN card, Logical address is the Internet Address orcommonly known as IP address that is used to uniquely & universally identify a device.
RARP- Reverse Address Resolution Protocol: It is used bya device on the network to find its Internet address when it knows its physical address.

Question sources

Data Communication & Networking practice questions · Question 30

Question 127 | Q01551

Which single option gives the complete set of listed algorithms or routing approaches usable in network-layer route design?

A. shortest path algorithm

B. distance vector routing

C. link state routing

D. all of the mentioned

Hint

Match the requested scope or data unit to the layer duties in the note; distinguish hop delivery from end-to-end process delivery.

Answer D: all of the mentioned

Distance-vector routing uses estimates received from neighboring routers. Link-state routing distributes link information and uses shortest-path computation to build routes. Therefore each named approach is usable in network-layer routing design. Because the question asks for the complete set, choosing any one named approach would omit other valid members; the combined response is the complete selection.

Why each choice is right or wrong

A - Incorrect: Shortest-path computation is usable, but this choice alone omits the other listed routing approaches.

B - Incorrect: Distance-vector routing is usable, but alone is an incomplete set.

C - Incorrect: Link-state routing is usable, but alone is an incomplete set.

D - Correct: All three approaches can be used, so the inclusive option gives the complete set.

Primary note proof

Study-note section NET30

Routing computes paths; forwarding chooses a next hop for an individual packet. Select the matching route with the longest prefix, then apply the routing system's tie-breaking criteria. A default /0 matches when nothing more specific does. Static routes are configured; dynamic protocols exchange reachability. Distance vector uses neighbor estimates, while link state distributes link information and computes shortest paths. Interior protocols operate within an autonomous system; BGP exchanges routes between systems.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 19 | lines 52-64

ROUTING AND ROUTING PROTOCOLS
Routing is the act of moving information across an internetwork from a source to a destination. At the heart of such protocol is the routing algorithm that determines the path for a packet.
• Routing requires a host or a router to have a routingtable which is constructed by the routing algorithm.
• There are wo kinds of routing algorithms (routing tables): nonadaptive (static) and adaptive (dynamic)
• And two kinds of protocols
o Interior routing protocols
o Exterior routing protocols

Data Communication and Computer Networking module | PDF page 48 | lines 10-21

In general, routing involves the network topology, or the setup of hardware, that can effectively relay data. Standard protocols help to identify the best routes for data and to ensure quality transmission. Individual pieces of hardware such as routers are referred to as —nodes‖ in the network. Different algorithms and protocols can be used to figure out how to best route data packets, and which nodes should be used. For example, some data packets travel according to a distance vector model that primarily uses distance as a factor, whereas others use Link-State Protocol, which involves other aspects of a —best path‖ for data.

Question sources

Data Communication & Networking practice questions · Question 31

Question 128 | Q01552

In a multi-destination scheme that carries an explicit list of multiple selected targets in each packet, which statements are incorrect as general descriptions? Select all that apply.

A. is same as broadcast routing

B. contains the list of all destinations

C. data is not sent by packets

D. there are multiple receivers

Hint

Use the cited note definitions to identify the requested function or scope, then check each alternative against that same rule.

Answer A, C: is same as broadcast routing; data is not sent by packets

A packet can carry a list identifying several selected destinations without addressing every destination in the broadcast scope. That makes universal equivalence with broadcasting false. The scheme is explicitly packet-based, so saying data are not sent by packets is also false. The list of targets and the presence of multiple receivers are true descriptions and therefore are not selected in this negative question.

Why each choice is right or wrong

A - Correct: Multi-destination delivery to listed targets is not necessarily broadcast to every destination in a scope.

B - Incorrect: A list of destinations is a supported multi-destination packet representation, making this statement correct.

C - Correct: NET30 explicitly describes multi-destination packets, contradicting the statement that data is not sent by packets.

D - Incorrect: Multiple targeted receivers are the defining destination-set property, so this statement is not incorrect.

Primary note proof

Study-note section NET30

> Flooding sends copies on eligible outgoing links with duplicate/lifetime controls; random walk picks a neighbor probabilistically. Unicast targets one destination, broadcast all in a scope, multicast a subscribed group and anycast one member sharing an address, normally nearest under routing metrics. Multi-destination packets can list multiple targets; this is not necessarily identical to broadcast. Group multicast trees use mechanisms such as reverse-path checks; Ethernet spanning tree is a different layer-2 mechanism.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 17 | lines 54-59

ICMP- Internet Control Message Protocol: It is a signaling mechanism used to inform the sender about datagram problemsthat occur during transit. It is used by intermediate devices.
IGMP- Internet Group Message Protocol: It is a mechanism that allows sending the same message to a group of recipients.

Data Communication and Computer Networking module | PDF page 15 | lines 41-61

Network Layer
• The network layer makes sure that the data is deliveredto the receiver despite multiple intermediate devices.
• The network layer at the sending side accepts data from the transport layer, divides it into packets, addsaddressing information in the header and passes it tothe data link layer.
• The network layer is responsible for source todestination of delivery of data.
• The network layer uses logical address commonlyknown as IP address to recognize devices on the network.
• Each packet is independent of the other and may travelusing different routes to reach the receiver hence may arrive out of turn at the receiver (Routing).
• The Network layer does not perform any flow controlor error control
• The main responsibility of Network Layer is transmission of packets from source to destination

Question sources

Data Communication & Networking practice questions · Question 32

Question 129 | Q01553

The network layer protocol for internet is _____

A. ethernet

B. internet protocol

C. hypertext transfer protocol

D. file transfer protocol

Hint

Match the requested scope or data unit to the layer duties in the note; distinguish hop delivery from end-to-end process delivery.

Answer B: internet protocol

IP is explicitly the network/Internetwork layer protocol. Evidence: PDF 17, 18, 26.

Why each choice is right or wrong

A - Incorrect: Ethernet is a network-access/LAN technology (PDF 17, 18, 26.)

B - Correct: Internet Protocol is the explicit network-layer protocol (PDF 17, 18, 26.)

C - Incorrect: HTTP is an application service in the port table (PDF 17, 18, 26.)

D - Incorrect: FTP is explicitly application file transfer (PDF 17, 18, 26.)

Primary note proof

Study-note section NET16

> IP supplies connectionless best-effort packet delivery, not end-to-end ordering or retransmission. IPv4 addresses are 32 bits. Its minimum header is 20 bytes and can grow to 60 bytes; it is not a 32-bit header. IHL counts 32-bit words; total length includes header and payload. TTL limits lifetime across routers; the protocol field identifies TCP, UDP or another upper-layer protocol.

Study-note section NET13

> Link-layer LLC identifies or multiplexes upper-layer protocols and may supply link control; MAC handles medium-dependent addressing/access and frame delivery. Network addressing belongs to layer 3. Ethernet, PPP and HDLC are link protocols. Frame headers may carry addresses and control/type fields; synchronization and exact framing depend on the protocol.

Study-note section NET21

> HTTP defines web request/response semantics; it is stateless, and a message body may be absent. HTTPS adds TLS protection. FTP transfers files using control and separate data connections; it is not the same protocol as SFTP. SMTP submits and relays mail; POP3 retrieves messages and IMAP accesses/synchronizes server mailboxes. Saying SMTP handles both sending and end-user mailbox retrieval is inaccurate.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 17 | lines 22-38

> Network Layer or IP
> Also called as the Internetwork Layer (IP). It holds the
> IP protocol which is a network layer protocol and is
> responsiblefor source to destination transmission of
> data.
> The Internetworking Protocol (IP) is a connection-less &
> unreliable protocol.

It is a best effort delivery service. i.e. there is no error checking in IP, it simply sends the data and relies on its underlying layers to get the data transmitted to the destination.Even if it is unreliable IP cannot be considered weak and useless; since it provides only the functionality that is requiredfor transmitting data thereby giving maximum efficiency.
Since there is no mechanism of error detection or correction in IP, there will be no delay introduced on a medium where thereis no error at all.

Data Communication and Computer Networking module | PDF page 18 | lines 27-32

Application Layer
The Application Layer is a combination of Session, Presentation & Application Layers of OSI models and defines high level protocols like File Transfer (FTP), Electronic Mail (SMTP), Virtual Terminal (TELNET), Domain Name Service (DNS), etc.

Data Communication and Computer Networking module | PDF page 26 | lines 14-28

medium. TCP/IP was designed to be independent of the network access method, frame format, and medium. In this way, TCP/IP can be used to connect differing network types. These include LAN technologies such as Ethernet and Token Ring and WAN technologies such as X.25 and Frame Relay. Independence from any specific network technology gives TCP/IP the ability to be adapted to new technologies such as Asynchronous Transfer Mode (ATM).
Network Access layer uses a physical address to identify hosts and to deliver data.
The Network Access layer PDU is called a frame. It contains the IP packet as well as a protocol header and trailer from this layer.

Question sources

Data Communication & Networking practice questions · Question 33

Question 130 | Q01554

ICMP is primarily used for _____

A. error and diagnostic functions

B. addressing

C. forwarding

D. routing

Hint

Use the cited note definitions to identify the requested function or scope, then check each alternative against that same rule.

Answer A: error and diagnostic functions

ICMP provides error reports, echo connectivity checks and timeout-based traceroute. These are error and diagnostic functions. Evidence: PDF 27, 17, 12.

Why each choice is right or wrong

A - Correct: Matches destination-unreachable, echo and timeout examples (PDF 27, 17, 12.)

B - Incorrect: ARP handles address resolution; ICMP is not the addressing scheme (PDF 27, 17, 12.)

C - Incorrect: Routers forward packets; ICMP reports conditions (PDF 27, 17, 12.)

D - Incorrect: A routing algorithm chooses paths; ICMP provides diagnostics rather than route choice (PDF 27, 17, 12.)

Primary note proof

Study-note section NET20

> ARP resolves an on-link IPv4 next hop to a link address, using a broadcast request and normally unicast reply. For an off-subnet target, ARP resolves the gateway, not the remote target's MAC. It bridges the network/link addressing boundary and is often classified at the link layer; calling ARP simply a network protocol uses a loose textbook convention. RARP reverses hardware-to-IP lookup; BOOTP/DHCP support boot configuration. ICMP reports errors and diagnostics; IGMP manages IPv4 multicast membership. These are separate companion protocols, not four pieces whose combination is IP.

Study-note section NET30

> Routing computes paths; forwarding chooses a next hop for an individual packet. Select the matching route with the longest prefix, then apply the routing system's tie-breaking criteria. A default /0 matches when nothing more specific does. Static routes are configured; dynamic protocols exchange reachability. Distance vector uses neighbor estimates, while link state distributes link information and computes shortest paths. Interior protocols operate within an autonomous system; BGP exchanges routes between systems.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 27 | lines 5-31

Internet Control Message Protocol (ICMP):
works at the Network layer and is used by IP for many different services. ICMP is a management protocol and messagingservice provider for IP. The following are some common events and messages that ICMP relates to:
Destination Unreachable: If a router can‘t send an IP datagram any further, it uses ICMP to send a message back to the sender, advising it of the situation.
Buffer Full: If a router‘s memory buffer for receiving incoming datagrams is full, it will use ICMP to send out this message until the congestion abates.
Hops: Each IP datagram is allotted a certain number of routers, called hops, to pass through. If it reaches its limitof hops before arriving at its destination, the last router to receive that datagram deletes it. The executioner router then uses ICMP to send an obituary message, informing the sending machine of the demise of its datagram.
Ping (Packet Internet Groper) uses ICMP echo messages to check the physical and logical connectivity of machineson a network.
Traceroute Using ICMP timeouts, Traceroute is used to discover the path a packet takes as it traverses an Internetwork.

Data Communication and Computer Networking module | PDF page 17 | lines 44-53

ARP - Address Resolution Protocol: It is used to resolve thephysical address of a device on a network, where its logical address is known.
Physical address is the 48 bit address that is imprinted on theNIC or LAN card, Logical address is the Internet Address orcommonly known as IP address that is used to uniquely & universally identify a device.
RARP- Reverse Address Resolution Protocol: It is used bya device on the network to find its Internet address when it knows its physical address.

Data Communication and Computer Networking module | PDF page 12 | lines 38-52

ROUTER: Router is a specialized network device used tointerconnect different types of network that uses different protocol.
Router allows the users to connect several LAN and WAN
• A LAN to another LAN

• A WAN to another WAN
• A LAN to the Internet
Routers use the routing table to determine how to forwardpackets.
• The list of routing tables provides directions to transfer the data to a particular network destination -various paths to forward the data.
• A router analyzes a destination IP address of a givenpacket and compares it with the routing table to decide the packet's next best path

Question sources

Data Communication & Networking practice questions · Question 34

Question 131 | Q01555

At a sending host, transport identifies data from different application endpoints using ports and forms segments or datagrams. To which OSI layer does it pass these units directly?

A. network layer

B. data link layer

C. application layer

D. physical layer

Hint

Match the requested scope or data unit to the layer duties in the note; distinguish hop delivery from end-to-end process delivery.

Answer A: network layer

On the sending path, transport creates segments or datagrams and hands them to the network layer for packet delivery. The network layer then uses the data-link layer, which in turn uses physical signaling. Ports distinguish application endpoints; this multiplexing does not merge unrelated applications into one undifferentiated TCP byte stream. The answer follows the immediate downward interface in the OSI stack.

Why each choice is right or wrong

A - Correct: The network layer immediately receives transport units on the sending path.

B - Incorrect: Data link is below network, not immediately below transport.

C - Incorrect: Application is above transport rather than its downward delivery target.

D - Incorrect: Physical is below both network and data link.

Primary note proof

Study-note section NET12

Sending proceeds from application data to transport segment/datagram, network packet, link frame and physical bits/symbols; receiving reverses the order. Each layer serves the layer above. A router removes a received link frame, inspects IP, and creates a new link frame for the next hop. MAC addresses usually change across routed hops; end-to-end IP addresses ordinarily remain until translation.

Study-note section NET18

TCP setup creates a logical transport connection, not a reserved physical circuit. Ports allow multiplexing separate applications over IP; they do not combine all applications into one TCP byte stream. Do not assign TCP reliability to all layer-4 protocols merely because the reference layer lists reliability as a possible service.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 16 | lines 2-17

• At the sending side, the transport layer receives data from the session layer, divides it into units called segments and sends it to the network layer.
• To ensure process to process delivery the transport layer makes use of port address to identify the data from the sending and receiving process.
• The data can be transported in a connection oriented or connectionless manner.
• The Transport layer is responsible for segmentation and reassembly of the message into segments which bear sequence numbers.
• The transport layer also carries out flow control and error control functions; but unlike data link layer these are end to end rather than node to node.
• The main responsibility of the transport layer is process to process delivery of the entire message

Data Communication and Computer Networking module | PDF page 15 | lines 41-61

Network Layer
• The network layer makes sure that the data is deliveredto the receiver despite multiple intermediate devices.
• The network layer at the sending side accepts data from the transport layer, divides it into packets, addsaddressing information in the header and passes it tothe data link layer.
• The network layer is responsible for source todestination of delivery of data.
• The network layer uses logical address commonlyknown as IP address to recognize devices on the network.

• Each packet is independent of the other and may travelusing different routes to reach the receiver hence may arrive out of turn at the receiver (Routing).
• The Network layer does not perform any flow controlor error control
• The main responsibility of Network Layer is transmission of packets from source to destination

Data Communication and Computer Networking module | PDF page 15 | lines 13-40

Data Link Layer
• The Data Link layer adds reliability to the physical layer by providing error detection and correction mechanisms.
• Framing: the Data Link layer receives the data from Network Layer and divides the stream of bits into fixed size manageable units called as Frames and sends it to the physical layer. On the receiver side, the data link layer receives the stream of bits from the physical layer and regroups them into frames and sends them to the Network layer.
• Physical Addressing: The Data link layer appends the physical address in the header of the frame before sending it to physical layer.
• Flow control: The data link layer makes sure that the sender sends the data at a speed at which the receiver canreceive it else if there is an overflow at the receiver sidethe data will be lost.
• Error Control: The data link layer imposes error control mechanism to identify lost or damaged frames, duplicateframes and then retransmit them.
• Access Control: The data link layer imposes access control mechanism to determine which device has right to send data in an multipoint connection setting.
• Main Responsibility: The main responsibility of the data link layer is hop to hop transmission of frames.

Question sources

Data Communication & Networking practice questions · Question 35

Question 132 | Q01556

Which of the following are transport layer protocols used in networking?

A. TCP and FTP

B. UDP and HTTP

C. TCP and UDP

D. HTTP and FTP

Hint

Match the requested scope or data unit to the layer duties in the note; distinguish hop delivery from end-to-end process delivery.

Answer C: TCP and UDP

TCP and UDP are explicitly transport protocols; FTP and HTTP are application services. Evidence: PDF 18, 18.

Why each choice is right or wrong

A - Incorrect: FTP makes this pair include an application protocol (PDF 18, 18.)

B - Incorrect: HTTP makes this pair include an application protocol (PDF 18, 18.)

C - Correct: Both are explicitly transport protocols (PDF 18, 18.)

D - Incorrect: Both are application services, not transport protocols (PDF 18, 18.)

Primary note proof

Study-note section NET17

> TCP offers a reliable ordered byte stream using sequence numbers, acknowledgments, retransmission and windows. Flow control protects the receiver; congestion control protects network capacity. UDP sends independent datagrams with ports and a checksum but no built-in setup, delivery guarantee, retransmission or ordering. Live interactive traffic may choose UDP when late data is less useful than lost data. Application protocols can add reliability over UDP.

Study-note section NET21

> HTTP defines web request/response semantics; it is stateless, and a message body may be absent. HTTPS adds TLS protection. FTP transfers files using control and separate data connections; it is not the same protocol as SFTP. SMTP submits and relays mail; POP3 retrieves messages and IMAP accesses/synchronizes server mailboxes. Saying SMTP handles both sending and end-user mailbox retrieval is inaccurate.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 18 | lines 9-21

> TCP - Transmission Control Protocol: TCP is a reliable
> connection-oriented, reliable protocol. i.e. a connection is

established between the sender and receiver before the data can be transmitted. It divides the data it receives from the upper layer into segments and tags a sequence number to each segment which is used at the receiving end for reordering of data.
UDP - User Datagram Protocol: UDP is a simple protocol used for process to process transmission. It is an unreliable, connectionless protocol for applications that do not require flow control or error control. It simply adds port address, checksum and length information to the data it receives from the upper layer.

Data Communication and Computer Networking module | PDF page 18 | lines 27-32

Application Layer
The Application Layer is a combination of Session, Presentation & Application Layers of OSI models and defines high level protocols like File Transfer (FTP), Electronic Mail (SMTP), Virtual Terminal (TELNET), Domain Name Service (DNS), etc.

Question sources

Data Communication & Networking practice questions · Question 36

Question 133 | Q01557

User datagram protocol is called connectionless because _____

A. all UDP packets are treated independently by transport layer

B. it sends data as a stream of related packets

C. it is received in the same order as sent order

D. it sends data very quickly

Hint

Identify the requested service or delivery guarantee, then distinguish application roles, transport behavior and address configuration.

Answer A: UDP treats datagrams independently without connection setup

Connectionless UDP sends independent datagrams without establishing a transport connection. NET17 explicitly separates this from TCP's reliable ordered byte stream. Fast transmission may be desirable but is not the definition of connectionlessness, and UDP itself does not preserve send order or combine datagrams into an ordered related stream.

Why each choice is right or wrong

A - Correct: Independent datagram treatment without built-in setup directly explains why UDP is connectionless.

B - Incorrect: An ordered related byte stream describes TCP's service rather than UDP's independent datagrams.

C - Incorrect: UDP provides no built-in ordering guarantee, so reception need not match transmission order.

D - Incorrect: Speed is not the defining condition; connectionlessness concerns the absence of connection establishment and associated state.

Primary note proof

Study-note section NET17

> TCP offers a reliable ordered byte stream using sequence numbers, acknowledgments, retransmission and windows. Flow control protects the receiver; congestion control protects network capacity. UDP sends independent datagrams with ports and a checksum but no built-in setup, delivery guarantee, retransmission or ordering. Live interactive traffic may choose UDP when late data is less useful than lost data. Application protocols can add reliability over UDP.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 18 | lines 9-21

> TCP - Transmission Control Protocol: TCP is a reliable connection-oriented, reliable protocol. i.e. a connection is established between the sender and receiver before the data can be transmitted. It divides the data it receives from the upper layer into segments and tags a sequence number to each segment which is used at the receiving end for reordering of data.
> UDP - User Datagram Protocol: UDP is a simple protocol used for process to process transmission. It is an unreliable, connectionless protocol for applications that do not require flow control or error control. It simply adds port address, checksum and length information to the data it receives from the upper layer.

Question sources

Data Communication & Networking practice questions · Question 37

Question 134 | Q01558

For one TCP connection, which single option gives the complete set of correct descriptions?

A. is a connection-oriented protocol

B. uses a three way handshake to establish a connection

C. receives data from application as a single stream

D. all of the mentioned

Hint

Identify the requested service or delivery guarantee, then distinguish application roles, transport behavior and address configuration.

Answer D: all of the mentioned

TCP establishes logical transport connection state through the SYN, SYN+ACK and ACK exchange. It then provides an ordered byte-stream service for that connection rather than preserving individual application message boundaries. All three descriptions apply to one TCP connection. Each individual response is therefore incomplete under the complete-set instruction, while the inclusive option collects all of the valid properties.

Why each choice is right or wrong

A - Incorrect: TCP is connection-oriented, but this choice alone omits its handshake and stream properties.

B - Incorrect: TCP uses a three-way handshake, but that alone is an incomplete set.

C - Incorrect: TCP accepts an application byte stream within a connection, but this alone is incomplete.

D - Correct: Connection orientation, three-way setup and a per-connection byte stream are all valid.

Primary note proof

Study-note section NET18

> TCP establishes state with SYN, SYN+ACK, then ACK. SYN consumes one sequence position even with no application bytes. An acknowledgment states the next expected sequence number. For client ISN=395 and server ISN=260: client sends SYN seq395; server sends SYN+ACK seq260 ack396; client sends ACK seq396 ack261. Later byte counts advance sequence numbers. FIN also consumes one sequence position.

Study-note section NET17

> TCP offers a reliable ordered byte stream using sequence numbers, acknowledgments, retransmission and windows. Flow control protects the receiver; congestion control protects network capacity. UDP sends independent datagrams with ports and a checksum but no built-in setup, delivery guarantee, retransmission or ordering. Live interactive traffic may choose UDP when late data is less useful than lost data. Application protocols can add reliability over UDP.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 18 | lines 9-21

TCP - Transmission Control Protocol: TCP is a reliable connection-oriented, reliable protocol. i.e. a connection is established between the sender and receiver before the data can be transmitted. It divides the data it receives from the upper layer into segments and tags a sequence number to each segment which is used at the receiving end for reordering of data.
UDP - User Datagram Protocol: UDP is a simple protocol used for process to process transmission. It is an unreliable, connectionless protocol for applications that do not require flow control or error control. It simply adds port address, checksum and length information to the data it receives from the upper layer.

Data Communication and Computer Networking module | PDF page 16 | lines 2-17

• At the sending side, the transport layer receives data from the session layer, divides it into units called segments and sends it to the network layer.
• To ensure process to process delivery the transport layer makes use of port address to identify the data from the sending and receiving process.
• The data can be transported in a connection oriented or connectionless manner.
• The Transport layer is responsible for segmentation and reassembly of the message into segments which bear sequence numbers.
• The transport layer also carries out flow control and error control functions; but unlike data link layer these are end to end rather than node to node.
• The main responsibility of the transport layer is process to process delivery of the entire message

Question sources

Data Communication & Networking practice questions · Question 38

Question 135 | Q01559

A _____ is a TCP name for a transport service access point.

A. port

B. pipe

C. node

D. protocol

Hint

Identify the requested service or delivery guarantee, then distinguish application roles, transport behavior and address configuration.

Answer A: port

Ports identify source/destination applications or processes for transport delivery, fitting a transport service access point in this question. Evidence: PDF 28, 16.

Why each choice is right or wrong

A - Correct: Port is the module application/process identifier (PDF 28, 16.)

B - Incorrect: Pipe is not the described TCP endpoint identifier (PDF 28, 16.)

C - Incorrect: Node is a network device rather than application endpoint (PDF 28, 16.)

D - Incorrect: Protocol names rules, not the numeric process endpoint (PDF 28, 16.)

Primary note proof

Study-note section NET17

> Ports identify transport endpoints; the application can choose a transport and request socket buffer sizes, subject to OS limits. A TCP connection is identified by source/destination IP and source/destination port, with TCP understood. IPv4 protocol numbers identify upper protocols; 80 is a usual HTTP port, not an IP protocol number. Clients often use ephemeral ports. SCTP is a reliable message-oriented transport with multiple streams.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 28 | lines 2-14

> TCP and UDP must use port numbers to communicate
> with the upper layers, because they‘re what keep track of
> different conversations crossing the network
> simultaneously. These port numbers identify the source
> and destination application or process in the TCP
> segment. There are 216 = 65,536 ports available.
> Well-known ports: The port numbers range from 0 to
> 1,023.
> Registered ports: The port numbers range from 1,024 to

49,151. Registered ports are used by applications or services that need to have consistent port assignments. Dynamic or private ports: The port numbers range from 49,152 to 65,535.

Data Communication and Computer Networking module | PDF page 16 | lines 2-17

• At the sending side, the transport layer receives data from the session layer, divides it into units called segments and sends it to the network layer.
• To ensure process to process delivery the transport layer makes use of port address to identify the data from the sending and receiving process.
• The data can be transported in a connection oriented or connectionless manner.
• The Transport layer is responsible for segmentation and reassembly of the message into segments which bear sequence numbers.
• The transport layer also carries out flow control and error control functions; but unlike data link layer these are end to end rather than node to node.
• The main responsibility of the transport layer is process to process delivery of the entire message

Question sources

Data Communication & Networking practice questions · Question 39

Question 136 | Q01560

Which phrase names the precise transport-layer endpoint-delivery responsibility in the OSI model?

A. application to application communication

B. process to process communication

C. node to node communication

D. man to man communication

Hint

Match the requested scope or data unit to the layer duties in the note; distinguish hop delivery from end-to-end process delivery.

Answer B: process to process communication

Transport provides process-to-process delivery, with ports identifying transport endpoints. Application-to-application communication is a broader description of what that service supports, but it does not name the precise endpoint-delivery term requested here. Hop or node-to-node frame delivery belongs to the data-link layer. Human communication describes an application purpose rather than the protocol endpoint responsibility used to distinguish the OSI layers.

Why each choice is right or wrong

A - Incorrect: Applications use transport, but this broad description does not name the precise process-delivery term requested.

B - Correct: Process-to-process is the precise transport endpoint-delivery responsibility.

C - Incorrect: Hop/node-to-node frame delivery is a link-layer responsibility rather than transport process delivery.

D - Incorrect: Human-to-human interaction is not the protocol endpoint service defining transport.

Primary note proof

Study-note section NET17

> Ports identify transport endpoints; the application can choose a transport and request socket buffer sizes, subject to OS limits. A TCP connection is identified by source/destination IP and source/destination port, with TCP understood. IPv4 protocol numbers identify upper protocols; 80 is a usual HTTP port, not an IP protocol number. Clients often use ephemeral ports. SCTP is a reliable message-oriented transport with multiple streams.

Study-note section NET14

> Controlled access uses polling, reservations or a token to grant turns; correctly coordinated access avoids contention collisions. Channelization divides frequency, time or code resources. Stop-and-wait sends one frame and waits for ACK, retransmitting on timeout; sequence bits distinguish duplicates. Sliding windows permit multiple unacknowledged frames. Link reliability/flow control is hop-local; transport reliability/flow control is end-to-end. Ethernet detects corruption but does not itself guarantee reliable delivery.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 16 | lines 2-17

> • At the sending side, the transport layer receives data from the session layer, divides it into units called segments and sends it to the network layer.
> • To ensure process to process delivery the transport layer makes use of port address to identify the data from the sending and receiving process.
> • The data can be transported in a connection oriented or connectionless manner.

• The Transport layer is responsible for segmentation and reassembly of the message into segments which bear sequence numbers.
• The transport layer also carries out flow control and error control functions; but unlike data link layer these are end to end rather than node to node.
• The main responsibility of the transport layer is process to process delivery of the entire message

Data Communication and Computer Networking module | PDF page 28 | lines 2-14

TCP and UDP must use port numbers to communicate with the upper layers, because they‘re what keep track of different conversations crossing the network simultaneously. These port numbers identify the source and destination application or process in the TCP segment. There are 216 = 65,536 ports available.
Well-known ports: The port numbers range from 0 to 1,023.
Registered ports: The port numbers range from 1,024 to 49,151. Registered ports are used by applications or services that need to have consistent port assignments.
Dynamic or private ports: The port numbers range from 49,152 to 65,535.

Question sources

Data Communication & Networking practice questions · Question 40

Question 137 | Q01561

A local telephone network is an example of a _____ network.

A. Packet switched

B. Circuit switched

C. Bit switched

D. Line switched

Hint

Use the cited note definitions to identify the requested function or scope, then check each alternative against that same rule.

Answer B: Circuit switched

Assuming the traditional local circuit telephone network, call setup creates a dedicated circuit and teardown releases it. This identifies circuit switching.

Why each choice is right or wrong

A - Incorrect: Packet switching is discrete packet communication

B - Correct: Circuit switching matches the traditional dedicated-call assumption

C - Incorrect: Bit switched is not a listed switching category

D - Incorrect: Line switched is not a listed switching category

Primary note proof

Study-note section NET31

Circuit switching sets up a path with reserved resources, transfers data, then releases it. Predictable allocated bandwidth trades against setup/blocking and wasted reservation during silence. A traditional telephone call is the standard example. Packet switching divides data into packets that share links statistically; queueing can add variable delay and loss. This does not make modern voice-over-packet impossible: buffering, scheduling and capacity planning manage it.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 20 | lines 12-26

Circuit Switching: In circuit switching, two
communicating stations are connected by a dedicated
communication path which consists of intermediate
nodes in the network and the links that connect these
nodes.
It involved the following three distinct steps
• Circuit Establishment: To establish an end-to-end
connection before any transfer of data.
• Data transfer: Transfer data is from the source to the
destination. The data may be analog or digital,
depending on the nature of the network. The
connection is generally full-duplex.
• Circuit disconnect: Terminate connection at the end
of data transfer. Signals must be propagated to
deallocate the dedicated resources.

Data Communication and Computer Networking module | PDF page 20 | lines 27-36

Message Switching:
Packet Switching: Packet switching was designed to
address the shortcomings of circuit switching in dealing with
data communication. Unlike circuit switching where
communication is continuous along a dedicated circuit, in
packet switching, communication is discrete in form of packets.
The three switching modes to choose from are:
• Cut-through

- Store-and-forward
- Fragment-free

Question sources

Data Communication & Networking practice questions · Question 41

Question 138 | Q01562

Most packet switches use this principle _____

A. Stop and wait

B. Store and forward

C. Store and wait

D. Stop and forward

Hint

Compare signal repetition, frame forwarding, packet routing and policy enforcement using the stated device or traffic assumptions.

Answer B: Store and forward

Packet store-and-forward means receiving the complete packet or frame before forwarding it. That is the switching principle named by B. Stop-and-wait is instead a reliability procedure that sends one frame and waits for acknowledgment. Cut-through alternatives exist, so the answer identifies the conventional principle without claiming every switch must use it.

Why each choice is right or wrong

A - Incorrect: Stop-and-wait is a link reliability/flow procedure involving acknowledgments, not the switching-buffering principle.

B - Correct: Store-and-forward buffers the full packet or frame before sending it on the next link.

C - Incorrect: Store and wait is not the defined switching principle named in NET31.

D - Incorrect: Stop and forward is not the defined receive-complete-then-forward switching procedure.

Primary note proof

Study-note section NET31

Datagram packets are forwarded independently. Virtual circuits establish forwarding state, but resource reservation is optional, not a necessary property of every virtual circuit. Message switching stores a complete message before forwarding, without a dedicated end-to-end path. Packet store-and-forward waits for the full packet/frame; cut-through starts after enough header arrives; fragment-free historically waits through the initial collision-sensitive portion. No routing algorithm guarantees that every packet always takes the geometrically shortest route.

Study-note section NET14

Controlled access uses polling, reservations or a token to grant turns; correctly coordinated access avoids contention collisions. Channelization divides frequency, time or code resources. Stop-and-wait sends one frame and waits for ACK, retransmitting on timeout; sequence bits distinguish duplicates. Sliding windows permit multiple unacknowledged frames. Link reliability/flow control is hop-local; transport reliability/flow control is end-to-end. Ethernet detects corruption but does not itself guarantee reliable delivery.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 20 | lines 27-36

Message Switching:
Packet Switching: Packet switching was designed to address the shortcomings of circuit switching in dealing with data communication. Unlike circuit switching where communication is continuous along a dedicated circuit, in packet switching, communication is discrete in form of packets.
The three switching modes to choose from are:
• Cut-through
• Store-and-forward
• Fragment-free

Question sources

Data Communication & Networking practice questions · Question 42

Question 139 | Q01563

Which is not a application layer protocol?

A. HTTP

B. SMTP

C. FTP

D. TCP

Hint

Match the requested scope or data unit to the layer duties in the note; distinguish hop delivery from end-to-end process delivery.

Answer D: TCP

TCP is explicitly transport, whereas SMTP/FTP and the HTTP service belong to the application side. Evidence: PDF 18, 18, 28.

Why each choice is right or wrong

A - Incorrect: HTTP appears as an application service in the port table (PDF 18, 18, 28.)

B - Incorrect: SMTP is in the application protocol list (PDF 18, 18, 28.)

C - Incorrect: FTP is explicitly application file transfer (PDF 18, 18, 28.)

D - Correct: TCP is explicitly a transport protocol (PDF 18, 18, 28.)

Primary note proof

Study-note section NET21

HTTP defines web request/response semantics; it is stateless, and a message body may be absent. HTTPS adds TLS protection. FTP transfers files using control and separate data connections; it is not the same protocol as SFTP. SMTP submits and relays mail; POP3 retrieves messages and IMAP accesses/synchronizes server mailboxes. Saying SMTP handles both sending and end-user mailbox retrieval is inaccurate.

Study-note section NET17

TCP offers a reliable ordered byte stream using sequence numbers, acknowledgments, retransmission and windows. Flow control protects the receiver; congestion control protects network capacity. UDP sends independent datagrams with ports and a checksum but no built-in setup, delivery guarantee, retransmission or ordering. Live interactive traffic may choose UDP when late data is less useful than lost data. Application protocols can add reliability over UDP.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 18 | lines 9-21

TCP - Transmission Control Protocol: TCP is a reliable connection-oriented, reliable protocol. i.e. a connection is established between the sender and receiver before the data can be transmitted. It divides the data it receives from the upper layer into segments and tags a sequence number to each segment which is used at the receiving end for reordering of data.
UDP - User Datagram Protocol: UDP is a simple protocol used for process to process transmission. It is an unreliable, connectionless protocol for applications that do not require flow control or error control. It simply adds port address, checksum and length information to the data it receives from the upper layer.

Data Communication and Computer Networking module | PDF page 18 | lines 27-32

Application Layer
The Application Layer is a combination of Session, Presentation & Application Layers of OSI models and defines high level protocols like File Transfer (FTP), Electronic Mail (SMTP), Virtual Terminal (TELNET), Domain Name Service (DNS), etc.

Data Communication and Computer Networking module | PDF page 28 | lines 32-45

Application Layer
The application layer in TCP/IP is equivalent to the combined session, presentation, and application layers in the OSI model and many protocols are defined at this layer.
The Process/Application Layer Protocols
• Telnet
• File Transfer Protocol (FTP)
• Network File System (NFS).
• Simple Mail Transfer Protocol (SMTP
• POP3 is used to receive mail.
• Simple Network Management Protocol (SNMP)
• Domain Name Service (DNS)
• Dynamic Host Configuration Protocol (DHCP)

Question sources

Data Communication & Networking practice questions · Question 43

Question 140 | Q01564

The packet of information at the application layer is called _____

A. Packet

B. Message

C. Segment

D. Frame

Hint

Match the requested scope or data unit to the layer duties in the note; distinguish hop delivery from end-to-end process delivery.

Answer B: Message

The module calls communicated information a message and transport receives upper-layer data before segmenting it. Message is the suitable upper/application unit among these options. Evidence: PDF 5, 16, 16, 15, 15.

Why each choice is right or wrong

A - Incorrect: Packet is network-layer terminology

B - Correct: Message names the communicated upper data

C - Incorrect: Segment is transport terminology

D - Incorrect: Frame is data-link terminology

Primary note proof

Study-note section NET12

Sending proceeds from application data to transport segment/datagram, network packet, link frame and physical bits/symbols; receiving reverses the order. Each layer serves the layer above. A router removes a received link frame, inspects IP, and creates a new link frame for the next hop. MAC addresses usually change across routed hops; end-to-end IP addresses ordinarily remain until translation.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 5 | lines 23-35

A Data Communication system has five components:-
• Message:- is the information to be communicated by the sender to the receiver.
• Sender The sender is any device that is capable of sending the data (message).
• Receiver: - is a device that the sender wants to communicate the data (message).
• Transmission Medium: - It is the path by which the message travels from sender to receiver. It can be wired or wireless and many subtypes in both.
• Protocol:- It is an agreed upon set or rules used by the sender and receiver to communicate data. Rules that govern data communication.

Data Communication and Computer Networking module | PDF page 16 | lines 43-47

Application Layer
• The application layer enables the user to communicate its data to the receiver by providing certain services.
• The main Responsibility of Application layer is to provide the user access to network resources.

Data Communication and Computer Networking module | PDF page 16 | lines 2-17

• At the sending side, the transport layer receives data from the session layer, divides it into units called segments and sends it to the network layer.
• To ensure process to process delivery the transport layer makes use of port address to identify the data from the sending and receiving process.
• The data can be transported in a connection oriented or connectionless manner.
• The Transport layer is responsible for segmentation and reassembly of the message into segments which bear sequence numbers.
• The transport layer also carries out flow control and error control functions; but unlike data link layer these are end to end rather than node to node.

• The main responsibility of the transport layer is process to process delivery of the entire message

Data Communication and Computer Networking module | PDF page 15 | lines 13-40

Data Link Layer
• The Data Link layer adds reliability to the physical layer by providing error detection and correction mechanisms.
• Framing: the Data Link layer receives the data from Network Layer and divides the stream of bits into fixed size manageable units called as Frames and sends it to the physical layer. On the receiver side, the data link layer receives the stream of bits from the physical layer and regroups them into frames and sends them to the Network layer.
• Physical Addressing: The Data link layer appends the physical address in the header of the frame before sending it to physical layer.
• Flow control: The data link layer makes sure that the sender sends the data at a speed at which the receiver canreceive it else if there is an overflow at the receiver sidethe data will be lost.
• Error Control: The data link layer imposes error control mechanism to identify lost or damaged frames, duplicateframes and then retransmit them.
• Access Control: The data link layer imposes access control mechanism to determine which device has right to send data in an multipoint connection setting.
• Main Responsibility: The main responsibility of the data link layer is hop to hop transmission of frames.

Data Communication and Computer Networking module | PDF page 15 | lines 41-61

Network Layer
• The network layer makes sure that the data is deliveredto the receiver despite multiple intermediate devices.
• The network layer at the sending side accepts data from the transport layer, divides it into packets, addsaddressing information in the header and passes it tothe data link layer.
• The network layer is responsible for source todestination of delivery of data.
• The network layer uses logical address commonlyknown as IP address to recognize

devices on the network.
• Each packet is independent of the other and may travelusing different routes to reach the receiver hence may arrive out of turn at the receiver (Routing).
• The Network layer does not perform any flow controlor error control
• The main responsibility of Network Layer is transmission of packets from source to destination

Question sources

Data Communication & Networking practice questions · Question 44

Question 141 | Q01565

Which one of the following is an architecture paradigms?

A. Peer to peer

B. Client-server

C. HTTP

D. Both Peer-to-Peer & Client-Server

Hint

Use the cited note definitions to identify the requested function or scope, then check each alternative against that same rule.

Answer D: Both Peer-to-Peer & Client-Server

The architecture section explicitly describes client-server and peer-to-peer; HTTP is a protocol rather than that resource-service arrangement. Evidence: PDF 24, 18.

Why each choice is right or wrong

A - Incorrect: Peer-to-peer is an architecture, but the combined option includes the other valid architecture (PDF 24, 18.)

B - Incorrect: Client-server is an architecture, but the combined option includes the other valid architecture (PDF 24, 18.)

C - Incorrect: HTTP is a protocol/service, not either listed architecture paradigm (PDF 24, 18.)

D - Correct: Both named architectures are explicitly described (PDF 24, 18.)

Primary note proof

Study-note section NET02

An intranet serves an organization internally; an extranet exposes selected services to approved outsiders. Neither term alone specifies geographic size. A client requests a service; a server

supplies it. Peer systems may perform both roles. Dedicated servers concentrate on service workloads but can still be clients of DNS, backup or update services. A ten-user cutoff is a teaching guideline, not a technical law. Centralization simplifies administration but creates dependencies; peer networks still need security.

Study-note section NET21

HTTP defines web request/response semantics; it is stateless, and a message body may be absent. HTTPS adds TLS protection. FTP transfers files using control and separate data connections; it is not the same protocol as SFTP. SMTP submits and relays mail; POP3 retrieves messages and IMAP accesses/synchronizes server mailboxes. Saying SMTP handles both sending and end-user mailbox retrieval is inaccurate.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 24 | lines 23-35

Network Architecture: based on the architecture
(where do the clients get the shared resources?),
networks can be categorized into three:
Client-Server Architecture: There can be one or
more systems acting as Server. Other being Client,
request the Server to serve requests. Servers take and
process request on clients‘ behalf.
Peer-to-Peer (Point-to-point): Two systems can be
connected Point-to-Point, or in other words back-to-
back fashion. They both reside on same level and
called peers.
There can be hybrid network which involves network
architecture of both the above types.

Data Communication and Computer Networking module | PDF page 18 | lines 27-32

Application Layer
The Application Layer is a combination of Session,
Presentation & Application Layers of OSI models and defines
high level protocols like File Transfer (FTP), Electronic Mail
(SMTP), Virtual Terminal (TELNET), Domain Name Service
(DNS), etc.

Question sources

Data Communication & Networking practice questions · Question 45

Question 142 | Q01566

Application developer has permission to decide the following on transport layer side

A. Transport layer protocol

B. Maximum buffer size

C. Both Transport layer protocol and Maximum buffer size

D. None of the mentioned

Hint

Match the requested scope or data unit to the layer duties in the note; distinguish hop delivery from end-to-end process delivery.

Answer C: Choose transport protocol and request buffer size, subject to OS limits

NET17 permits an application to choose its transport protocol and request socket-buffer sizes. In that application-configuration sense, C combines both choices. “Maximum buffer size” must mean the requested socket limit, not authority to override the operating system’s enforced maximum; the note explicitly makes the request subject to OS limits.

Why each choice is right or wrong

A - Incorrect: Choosing a transport is permitted, but this option omits the also-permitted socket-buffer size request.

B - Incorrect: A buffer limit can be requested subject to OS limits, but this omits transport-protocol choice.

C - Correct: Both settings can be selected/requested by the application, with the buffer size constrained by the operating system.

D - Incorrect: At least transport choice and buffer-size requests are explicitly permitted, so none is false.

Primary note proof

Study-note section NET17

> Ports identify transport endpoints; the application can choose a transport and request socket buffer sizes, subject to OS limits. A TCP connection is identified by source/destination IP and source/destination port, with TCP understood. IPv4 protocol numbers identify upper protocols; 80 is a usual HTTP port, not an IP protocol number. Clients often use ephemeral ports. SCTP is a reliable message-oriented transport with multiple streams.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 18 | lines 9-21

> TCP - Transmission Control Protocol: TCP is a reliable
> connection-oriented, reliable protocol. i.e. a connection is
> established between the sender and receiver before the data can

be transmitted. It divides the data it receives from the upper layer into segments and tags a sequence number to each segment which is used at the receiving end for reordering of data.
UDP - User Datagram Protocol: UDP is a simple protocol used for process to process transmission. It is an unreliable, connectionless protocol for applications that do not require flow control or error control. It simply adds port address, checksum and length information to the data it receives from the upper layer.

Data Communication and Computer Networking module | PDF page 28 | lines 2-14

TCP and UDP must use port numbers to communicate with the upper layers, because they‘re what keep track of different conversations crossing the network simultaneously. These port numbers identify the source and destination application or process in the TCP segment. There are 216 = 65,536 ports available.
Well-known ports: The port numbers range from 0 to 1,023.
Registered ports: The port numbers range from 1,024 to 49,151. Registered ports are used by applications or services that need to have consistent port assignments.
Dynamic or private ports: The port numbers range from 49,152 to 65,535.

Question sources

Data Communication & Networking practice questions · Question 46

Question 143 | Q01567

Using “end-to-end” for application service and “process-to-process” for the transport service beneath it, which service does the application layer offer?

A. End to end

B. Process to process

C. Both End to end and Process to process

D. None of the mentioned

Hint

Match the requested scope or data unit to the layer duties in the note; distinguish hop delivery from end-to-end process delivery.

Answer A: End to end

The question explicitly separates an application service from the underlying transport service. The note describes end-to-end application service as building on process-to-process transport. Under those named scopes, the application layer offers the end-to-end service, while process delivery identifies the transport boundary. Combining both would collapse the distinction being tested; none of the mentioned fails because the application-service term is present.

Why each choice is right or wrong

A - Correct: End-to-end is the stated application-service scope.

B - Incorrect: Process-to-process names the underlying transport service in this question.

C - Incorrect: The combination assigns the underlying transport-service term to the application layer, contrary to the stated distinction.

D - Incorrect: The stated application-service term is offered in A.

Primary note proof

Study-note section NET19

> The four-layer TCP/IP model folds OSI layers 5-7 into application, retains transport, calls layer 3 Internet, and combines link/physical as network access. A model is a guide to functions, not a guarantee that every application gets a reliable network. Distinguish end-to-end application service from its underlying process-to-process transport.

Study-note section NET17

> Ports identify transport endpoints; the application can choose a transport and request socket buffer sizes, subject to OS limits. A TCP connection is identified by source/destination IP and source/destination port, with TCP understood. IPv4 protocol numbers identify upper protocols; 80 is a usual HTTP port, not an IP protocol number. Clients often use ephemeral ports. SCTP is a reliable message-oriented transport with multiple streams.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 16 | lines 43-47

> Application Layer
> • The application layer enables the user to communicate
> its data to the receiver by providing certain services.
> • The main Responsibility of Application layer is to
> provide the user access to network resources.

Data Communication and Computer Networking module | PDF page 16 | lines 2-17

> • At the sending side, the transport layer receives data
> from the session layer, divides it into units called
> segments and sends it to the network layer.
> • To ensure process to process delivery the transport
> layer makes use of port address to identify the data

from the sending and receiving process.
• The data can be transported in a connection oriented or connectionless manner.
• The Transport layer is responsible for segmentation and reassembly of the message into segments which bear sequence numbers.
• The transport layer also carries out flow control and error control functions; but unlike data link layer these are end to end rather than node to node.
• The main responsibility of the transport layer is process to process delivery of the entire message

Question sources

Data Communication & Networking practice questions · Question 47

Question 144 | Q01568

To deliver a message to the correct application program running on a host, the _____ address must be consulte
d.

A. IP

B. MAC

C. Port

D. None of the mentioned

Hint

Use the cited note definitions to identify the requested function or scope, then check each alternative against that same rule.

Answer C: Port

Port numbers explicitly identify the destination application/process, while IP identifies an interface and MAC a local physical endpoint. Evidence: PDF 28, 18, 17.

Why each choice is right or wrong

A - Incorrect: IP identifies the host interface, not which program (PDF 28, 18, 17.)

B - Incorrect: MAC identifies a local physical interface, not which program (PDF 28, 18, 17.)

C - Correct: Port identifies the process/application (PDF 28, 18, 17.)

D - Incorrect: None fails because the port option is present (PDF 28, 18, 17.)

Primary note proof

Study-note section NET17

Ports identify transport endpoints; the application can choose a transport and request socket buffer sizes, subject to OS limits. A TCP connection is identified by source/destination IP and source/destination port, with TCP understood. IPv4 protocol numbers identify upper protocols; 80 is a usual HTTP port, not an IP protocol number. Clients often use ephemeral ports. SCTP is a reliable message-oriented transport with multiple streams.

Study-note section NET-S06

An IP address identifies a network interface rather than limiting a whole computer to one address. A computer or router can have several interfaces and addresses. Under a supplied IPv4 prefix, leading bits identify the network and the remaining bits identify an address within that network; a MAC address is a separate link-layer identifier.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 28 | lines 2-14

TCP and UDP must use port numbers to communicate
with the upper layers, because they‘re what keep track of
different conversations crossing the network
simultaneously. These port numbers identify the source
and destination application or process in the TCP
segment. There are 216 = 65,536 ports available.
Well-known ports: The port numbers range from 0 to
1,023.
Registered ports: The port numbers range from 1,024 to
49,151. Registered ports are used by applications or
services that need to have consistent port assignments.
Dynamic or private ports: The port numbers range from
49,152 to 65,535.

Data Communication and Computer Networking module | PDF page 18 | lines 45-54

IP addresses: IP address uniquely identifies a device on the
Internet. Every host and router on the Internet has an IP address,
which encodes its network number and host number.
• The combination is unique: in principle, no two
machines on the Internet have the same IP address.
• An IPv4 address is 32 bits long
• They are used in the Source address and Destination
address fields of IP packets.
• An IP address does not refer to a host but it refers to a
network interface.

Data Communication and Computer Networking module | PDF page 17 | lines 44-53

ARP - Address Resolution Protocol: It is used to
resolve thephysical address of a device on a network,
where its logical address is known.
Physical address is the 48 bit address that is imprinted

on theNIC or LAN card, Logical address is the Internet Address orcommonly known as IP address that is used to uniquely & universally identify a device.
RARP- Reverse Address Resolution Protocol: It is used bya device on the network to find its Internet address when it knows its physical address.

Question sources

Data Communication & Networking practice questions · Question 48

Question 145 | Q01572

In TCP connection establishment procedure, if a client chooses Initial Sequence Number of 395, and server chooses 260, then:

A. The 1st segment sent will contain sequence number of 396

B. The 2nd segment sent will contain acknowledgement number of 261

C. The 3rd segment sent will contain sequence number of 261

D. The 2nd segment sent will contain acknowledgement number of 396

E. The 2nd segment sent will contain sequence number of 395

F. The 3rd segment sent will contain acknowledgement number of 396

Hint

Trace the handshake in order, keeping each endpoint's sequence and acknowledgment fields separate.

Answer D: Second segment acknowledgment number 396

SYN consumes one sequence position. The first segment is client SYN seq395. The server's second segment is SYN+ACK seq260 ack396, acknowledging the client SYN. The third is client ACK seq396 ack261. Comparing those fields shows only D matches; sequence numbers and acknowledgment numbers must not be swapped between endpoints.

Why each choice is right or wrong

A - Incorrect: The first client SYN uses its initial sequence number 395, not the next position 396.

B - Incorrect: The second segment acknowledges the client SYN with 396; 261 is the later acknowledgment of the server SYN.

C - Incorrect: The third segment's sequence number is the client's next position 396, not the server acknowledgment value 261.

D - Correct: The server's SYN+ACK acknowledges client ISN 395 plus one, giving 396.

E - Incorrect: The second segment is sent by the server with its own sequence number 260.

F - Incorrect: The third segment acknowledges server ISN 260 plus one, giving 261 rather than 396.

Primary note proof

Study-note section NET18

TCP establishes state with SYN, SYN+ACK, then ACK. SYN consumes one sequence position even with no application bytes. An acknowledgment states the next expected sequence number. For client ISN=395 and server ISN=260: client sends SYN seq395; server sends SYN+ACK seq260 ack396; client sends ACK seq396 ack261. Later byte counts advance sequence numbers. FIN also consumes one sequence position.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 18 | lines 9-21

TCP - Transmission Control Protocol: TCP is a reliable connection-oriented, reliable protocol. i.e. a connection is established between the sender and receiver before the data can be transmitted. It divides the data it receives from the upper layer into segments and tags a sequence number to each segment which is used at the receiving end for reordering of data.
UDP - User Datagram Protocol: UDP is a simple protocol used for process to process transmission. It is an unreliable, connectionless protocol for applications that do not require flow control or error control. It simply adds port address, checksum and length information to the data it receives from the upper layer.

Data Communication and Computer Networking module | PDF page 16 | lines 2-17

• At the sending side, the transport layer receives data from the session layer, divides it into units called segments and sends it to the network layer.
• To ensure process to process delivery the transport layer makes use of port address to identify the data from the sending and receiving process.
• The data can be transported in a connection oriented or connectionless manner.
• The Transport layer is responsible for segmentation and reassembly of the message into segments which bear sequence numbers.
• The transport layer also carries out flow control and error control functions; but unlike data link layer these are end to end rather than node to node.
• The main responsibility of the transport layer is process to process delivery of the entire message

Question sources

Mock exam 3 · Question 4

Question 146 | Q01573

For IPv4 when fragmentation is permitted, which option gives the complete set of nodes that may fragment packets and the location of reassembly?

A. Fragment at the source host; re-assemble at the destination host

B. Fragment at the source host and routers; re-assemble at the destination host

C. Fragment at the source host and routers; re-assemble at the routers and destination host

D. Fragment at the source host; re-assemble at the routers and destination host

E. IP does not support Fragmentation and Re-assembly.

Hint

Separate address width, syntax, reserved scope and the supplied prefix or historical classful convention.

Answer B: Fragment at the source host and routers; re-assemble at the destination host

IPv4 permits both the source and a router to fragment packets when fragmentation is allowed and an outgoing MTU requires it. The destination reassembles the fragments. Source-only fragmentation omits a permitted IPv4 case; it instead resembles the IPv6 restriction. Adding intermediate-router reassembly is incorrect. Naming IPv4 and asking for the complete permitted set makes the version-specific distinction explicit.

Why each choice is right or wrong

A - Incorrect: A source may fragment, but this option omits permitted IPv4 router fragmentation.

B - Correct: IPv4 sources and routers may fragment; only the destination reassembles.

C - Incorrect: Neither cited IP fragmentation rule places reassembly at intermediate routers.

D - Incorrect: Destination reassembly is required; the additional router reassembly claim is unsupported for either version.

E - Incorrect: Both version-specific rules support fragmentation and reassembly, although the allowed fragmenting nodes differ.

Primary note proof

Study-note section NET16

> The IPv4 checksum protects its header; IP does not lack error checking altogether. Identification, flags and offset support fragmentation. IPv4 sources and routers may fragment when allowed; reassembly occurs at the destination. If DF is set and the next MTU is too small, forwarding fails and an ICMP diagnostic may be returned.

Study-note section NET23

IPv6 has 128-bit hexadecimal addresses, flexible prefixes and no IPv4-style broadcast. Sources, not routers, fragment IPv6 packets. IPv6 does not automatically encrypt traffic or make authentication unnecessary. Compare IPv6's larger 128-bit address space and encryption support separately; specify the property being evaluated.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 15 | lines 41-61

Network Layer
• The network layer makes sure that the data is deliveredto the receiver despite multiple intermediate devices.
• The network layer at the sending side accepts data from the transport layer, divides it into packets, addsaddressing information in the header and passes it tothe data link layer.
• The network layer is responsible for source todestination of delivery of data.
• The network layer uses logical address commonlyknown as IP address to recognize devices on the network.
• Each packet is independent of the other and may travelusing different routes to reach the receiver hence may arrive out of turn at the receiver (Routing).
• The Network layer does not perform any flow controlor error control
• The main responsibility of Network Layer is transmission of packets from source to destination

Data Communication and Computer Networking module | PDF page 18 | lines 45-54

IP addresses: IP address uniquely identifies a device on the Internet. Every host and router on the Internet has an IP address, which encodes its network number and host number.
• The combination is unique: in principle, no two machines on the Internet have the same IP address.
• An IPv4 address is 32 bits long
• They are used in the Source address and Destination address fields of IP packets.
• An IP address does not refer to a host but it refers to a network interface.

Question sources

Mock exam 3 · Question 5

Question 147 | Q01574

Packets in one TCP connection can be distinguished from packets in another TCP connection by:

A. Source port, destination port, protocol number

B. Source IP address, destination IP address, protocol number

C. Source port, destination port, source IP address, destination IP address

D. Source IP address, destination IP address

E. Source port, destination port

F. Protocol number

Hint

Identify the requested service or delivery guarantee, then distinguish application roles, transport behavior and address configuration.

Answer C: Both IP addresses and both port numbers

All packets under discussion are already TCP, so their protocol identity is common. Distinguishing arbitrary simultaneous connections needs the endpoint four-tuple: source IP, destination IP, source port and destination port. Addresses alone cannot distinguish separate applications between the same hosts; ports alone can repeat between different hosts. C supplies all four required fields.

Why each choice is right or wrong

A - Incorrect: Ports and protocol can repeat between different host pairs, so this omits necessary IP addresses.

B - Incorrect: Two hosts can have several simultaneous TCP connections; addresses and TCP protocol alone do not distinguish them.

C - Correct: The source/destination IP addresses and source/destination ports form the TCP connection four-tuple.

D - Incorrect: An IP-address pair cannot distinguish multiple connections between the same two hosts.

E - Incorrect: The same source/destination port pair can be used with different IP-address endpoints.

F - Incorrect: Every connection in the stem uses TCP, so protocol number alone distinguishes none of them.

Primary note proof

Study-note section NET17

> Ports identify transport endpoints; the application can choose a transport and request socket buffer sizes, subject to OS limits. A TCP connection is identified by source/destination IP and source/destination port, with TCP understood. IPv4 protocol numbers identify upper protocols; 80 is a usual HTTP port, not an IP protocol number. Clients often use ephemeral ports. SCTP is a reliable message-oriented transport with multiple streams.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 28 | lines 2-14

TCP and UDP must use port numbers to communicate with the upper layers, because they‘re what keep track of different conversations crossing the network simultaneously. These port numbers identify the source and destination application or process in the TCP segment. There are 216 = 65,536 ports available.
Well-known ports: The port numbers range from 0 to 1,023.
Registered ports: The port numbers range from 1,024 to 49,151. Registered ports are used by applications or services that need to have consistent port assignments.
Dynamic or private ports: The port numbers range from 49,152 to 65,535.

Data Communication and Computer Networking module | PDF page 18 | lines 45-54

IP addresses: IP address uniquely identifies a device on the Internet. Every host and router on the Internet has an IP address, which encodes its network number and host number.
• The combination is unique: in principle, no two machines on the Internet have the same IP address.
• An IPv4 address is 32 bits long
• They are used in the Source address and Destination address fields of IP packets.
• An IP address does not refer to a host but it refers to a network interface.

Data Communication and Computer Networking module | PDF page 18 | lines 9-21

TCP - Transmission Control Protocol: TCP is a reliable connection-oriented, reliable protocol. i.e. a connection is established between the sender and receiver before the data can be transmitted. It divides the data it receives from the upper layer into segments and tags a sequence number to each segment which is used at the receiving end for reordering of data.
UDP - User Datagram Protocol: UDP is a simple protocol used for process to process transmission. It is an unreliable, connectionless protocol for applications that do not require flow control or error control. It simply adds port address, checksum and length information to the data it receives from the upper layer.

Question sources

Mock exam 3 · Question 6

Question 148 | Q01630

Compared to other common topologies in LANs (such as bus, mesh, ring), which of the following is a disadvantage of using a star topology for LAN?

A. Poor performance due to sharing of point-to-multipoint links between users

B. Failure of a single station results in no stations being able to communicate

C. Failure of a single link results in no stations being able to communicate

D. Each station requires many network interfaces

E. Too many links needed in the network

F. Failure of a special node results in no stations being able to communicate

Hint

Draw the links and identify shared components, alternate paths and the effect of the specified failure or growth requirement.

Answer F: Failure of a special node results in no stations being able to communicate

The star description explicitly calls its hub/switch a single point of failure: failure of that central device brings the whole system down. Ordinary station/link failure is isolated. Evidence: PDF 23, 23, 23, 23.

Why each choice is right or wrong

A - Incorrect: Star has separate central links, not the bus shared-backbone defect (PDF 23, 23, 23, 23.)

B - Incorrect: Failure of an ordinary station does not remove the central device (PDF 23, 23, 23, 23.)

C - Incorrect: The module says a link failure affects only its attached device (PDF 23, 23, 23, 23.)

D - Incorrect: Many interfaces per station is the full-mesh burden (PDF 23, 23, 23, 23.)

E - Incorrect: Star uses more cable than bus/ring but less than mesh, so this is not the distinctive universal comparison (PDF 23, 23, 23, 23.)

F - Correct: The special central node is explicitly a single point of failure (PDF 23, 23, 23, 23.)

Primary note proof

Study-note section NET08

> Bus uses a shared backbone; an unterminated break can disrupt the segment. Star connects endpoints through a central device: one edge failure isolates that endpoint, whereas central failure affects the star. Ring forms a loop; basic single rings are vulnerable to a break, while protected dual rings differ. Token passing is associated with Token Ring but is an access method, not a necessary property of every ring. Tree is hierarchical; hybrid combines arrangements.

Study-note section NET08

A full undirected mesh of n nodes needs n(n-1)/2 links and n-1 interfaces per node. For 50 nodes: 50×49/2=1225 links. Redundant paths improve fault tolerance at greater cable and interface cost.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 23 | lines 19-34

Star Topology: in this topology, each node is connected directly to a central device called a hub or a switch. Data on a star network passes through the central device (switch) before continuing to its destination. The central device manages and controls all functions of the network. This configuration is common with twisted pair cable. RJ-45 Connectors are used to connect the cable to the Network Interface Card (NIC) of each computer. Its advantages include, ease of installation and reconfiguration, robust (ease of fault identification and isolation), link failure only affects device(s) connected to that link, and is less expensive than mesh. Its drawbacks include more cable requirements (than bus and ring) and single point of failure (if central device fail, the whole system will be down).

Data Communication and Computer Networking module | PDF page 23 | lines 45-53

Mesh Topology: in this topology devices are connected with many redundant interconnections between network nodes. In a full mesh topology, every node has a connection to every other node in the network, which makes it the most expensive topology over all the other topologies. The number of cables grows fast as the number of nodes increases, and it can be calculated by using the general formula ((n (n - 1)) /2), where n is the number of nodes in the

Data Communication and Computer Networking module | PDF page 23 | lines 4-18

Bus Topology: in this topology all devices are connected to a central cable, called the bus or backbone, which is terminated at its ends. The purpose of the terminators is to stop the signal from bouncing, thereby clearing the cable so that other computers can send data. Message transmitted along the Bus is visible to all computers connected to the backbone cable. As the message arrives at each workstation, the workstation checks the destination address contained in the message either to process or drop the packet if it matches or not respectively. Its

advantages are, ease of installation and less amount of cable requirement. Its main drawback is, the entire network will be shut down if there is a break in the main cable.

Data Communication and Computer Networking module | PDF page 23 | lines 35-44

Ring Topology: in this topology, all devices are connected to one another in the shape of a closed loop, so that each device is connected directly to two other devices, one on either side of it. Some of its advantages include, easy to install and reconfigure, less expensive (than mesh), and performance is even despite the number of users. Its cons include, break in the ring (such as a disabled station) can disable the entire network, and limitations on media and traffic (limitation on ring length and number of devices).

Question sources

Mock exam 2 · Question 19

Question 149 | Q01631

For IPv4 networks, distinguish interface IP addresses, transport port numbers and the IPv4 Protocol header field. Which statement is true?

A. The protocol number commonly used by web server applications is 80

B. Every application must use a well-known port number

C. Each host and router in the Internet has only a single IP address

D. Client applications may dynamically select port numbers

E. A protocol number is used to indicate the version of IP being used

Hint

Identify the requested service or delivery guarantee, then distinguish application roles, transport behavior and address configuration.

Answer D: Client applications may dynamically select port numbers

Client applications commonly use dynamically selected ephemeral ports. Ports identify transport endpoints, whereas the IPv4 Protocol field identifies the carried upper-layer protocol, such as TCP or UDP. The separate Version field identifies the IP version. Port 80 is a usual HTTP service port, not an IP protocol number. Hosts and routers can have multiple addressed interfaces, so they are not restricted to one IP address.

Why each choice is right or wrong

A - Incorrect: 80 is a usual HTTP port number, not the IPv4 Protocol value for HTTP.

B - Incorrect: Clients may use ephemeral ports, so a well-known port is not mandatory for every application.

C - Incorrect: A device can have multiple addressed interfaces and therefore multiple IP addresses.

D - Correct: Clients may dynamically select ephemeral transport ports.

E - Incorrect: The IPv4 Protocol field identifies the upper-layer protocol; the Version field identifies the IP version.

Primary note proof

Study-note section NET-S06

> An IP address identifies a network interface rather than limiting a whole computer to one address. A computer or router can have several interfaces and addresses. Under a supplied IPv4 prefix, leading bits identify the network and the remaining bits identify an address within that network; a MAC address is a separate link-layer identifier.

Study-note section NET-S06

> TCP and UDP port fields are 16 bits, allowing numbers from 0 through 65535. Well-known ports are 0-1023, registered ports are 1024-49151, and dynamic/private ports are 49152-65535. Client endpoints can use dynamically selected ports instead of every application requiring a well-known assignment. These port numbers are distinct from the IP version and upper-protocol fields.

Study-note section NET16

> IP supplies connectionless best-effort packet delivery, not end-to-end ordering or retransmission. IPv4 addresses are 32 bits. Its minimum header is 20 bytes and can grow to 60 bytes; it is not a 32-bit header. IHL counts 32-bit words; total length includes header and payload. TTL limits lifetime across routers; the protocol field identifies TCP, UDP or another upper-layer protocol.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 28 | lines 2-14

> TCP and UDP must use port numbers to communicate
> with the upper layers, because they‘re what keep track of
> different conversations crossing the network
> simultaneously. These port numbers identify the source
> and destination application or process in the TCP
> segment. There are 216 = 65,536 ports available.
> Well-known ports: The port numbers range from 0 to
> 1,023.
> Registered ports: The port numbers range from 1,024 to
> 49,151. Registered ports are used by applications or
> services that need to have consistent port assignments.
> Dynamic or private ports: The port numbers range from
> 49,152 to 65,535.

Data Communication and Computer Networking module | PDF page 28 | lines 23-31

Telnet 23 SNMP 161
SMTP 25 TFTP 69
HTTP 80 DNS 53
FTP 21 POP3 110
DNS 53 DHCP 68
HTTPS 443 NTP 123
SSH 22 RPC 530
Table. Sample TCP and UDP port numbers from well-known category

Data Communication and Computer Networking module | PDF page 18 | lines 45-54

IP addresses: IP address uniquely identifies a device on the Internet. Every host and router on the Internet has an IP address, which encodes its network number and host number.
• The combination is unique: in principle, no two machines on the Internet have the same IP address.
• An IPv4 address is 32 bits long
• They are used in the Source address and Destination address fields of IP packets.
• An IP address does not refer to a host but it refers to a network interface.

Question sources

Mock exam 2 · Question 20

Question 150 | Q01632

If you would like to give IP address to 57 hosts from your IP prefix which subnet mask do you use most effectively?

A. 255.255.255.248

B. 255.255.255.240

C. 255.255.255.224

D. 255.255.255.128

E. 255.255.255.192

Hint

Convert the mask to a prefix, separate network and host bits, and apply the relevant subnet-count or usable-host rule.

Answer E: 255.255.255.192

For 57 hosts choose the smallest offered block with at least 57 total addresses: /26 (192=11000000) has 64. The next smaller /27 has only 32, and /25 wastes twice the space. Even the conventional two reserved addresses leave /26 sufficient. Evidence: PDF 19, 19.

Why each choice is right or wrong

A - Incorrect: 248 gives only eight total addresses (PDF 19, 19.)

B - Incorrect: 240 gives only 16 (PDF 19, 19.)

C - Incorrect: 224 gives only 32 (PDF 19, 19.)

D - Incorrect: 128 gives 128 and uses more space than necessary (PDF 19, 19.)

E - Correct: 192 gives 64, the smallest offered sufficient block (PDF 19, 19.)

Primary note proof

Study-note section NET26

> For H hosts, choose the smallest h satisfying 2^h-2≥H, then p=32-h. For 24 hosts use /27; 52 or 57 use /26; 100 use /25; 500 use /23. For at least six equal subnets choose b=3. A Class C /24 split to /27 yields eight subnets. Always check both the number of subnets and the host capacity.

Study-note section NET24

> A /p IPv4 prefix has p leading one bits followed by 32-p zeros. Partial octet masks are 128,192,224,240,248,252,254. /19 is 255.255.224.0; /20 is 255.255.240.0; /21 is 255.255.248.0, correcting the study guide’s 255.248.0.0 mistake.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 19 | lines 2-22

> Address Space: An address space is the total
> number ofaddresses used by the protocol.
> • If a protocol uses N bits to define an address,
> the address space is 2N
> because each bit can
> have twodifferent values (0 or 1) and N bits
> can have 2N values.
> • IPv4 uses 32-bit addresses, which means that
> the address space is 232 or 4,294,967,296
> (more than 4billion).
> Notations: There are two notations to show an IPv4 address:
> • Binary notation: The IPv4 address is displayed
> as 32bits. ex. 11000001 10000011 00011011
> 11111111
> • Dotted decimal notation: To make the IPv4
> address easier to read, Internet addresses are
> usually written in decimal form with a decimal

point (dot) separatingthe bytes. Each byte (octet) is 8 bits hence each number in dotted-decimal notation is a value rangingfrom 0 to 255. Ex. 129.11.11.239

Data Communication and Computer Networking module | PDF page 19 | lines 23-36

Classful addressing : In classful addressing, the addressspace is divided into five classes: A, B, C, D, and E.
• Netid and Hostid In classful addressing, an IP addressin class A, B, or C is divided into netid and hostid.
Subnetting: It allows a network to be split into several parts for internal use but still act like a single network to the outsideworld.
• To implement subnetting, the router needs a subnet mask that indicates the split between network + subnet number and host. Ex. 255.255.252.0/22. A‖/22‖ to indicate that the subnet mask is 22 bits long.

Question sources

Mock exam 2 · Question 21

Question 151 | SM0021

Which one of the following is NOT correct about POP3 and SMTP?

A. A sender can send email using SMTP

B. Both are application layer protocols

C. A sender can receive emails using POP3

D. Both are network layer protocols

Hint

Use the cited note definitions to identify the requested function or scope, then check each alternative against that same rule.

Answer D: Both are network layer protocols

The application-layer list includes SMTP and POP3; POP3 is explicitly for receiving mail. They are not network-layer protocols. Evidence: PDF 28, 18.

Why each choice is right or wrong

A - Incorrect: SMTP mail transfer supports sending (PDF 28, 18.)

B - Incorrect: Both appear in the application list (PDF 28, 18.)

C - Incorrect: Receiving via POP3 matches the explicit receive-mail statement (PDF 28, 18.)

D - Correct: Calling both network-layer protocols contradicts the layer list (PDF 28, 18.)

Primary note proof

Study-note section NET21

HTTP defines web request/response semantics; it is stateless, and a message body may be absent. HTTPS adds TLS protection. FTP transfers files using control and separate data connections; it is not the same protocol as SFTP. SMTP submits and relays mail; POP3 retrieves messages and IMAP accesses/synchronizes server mailboxes. Saying SMTP handles both sending and end-user mailbox retrieval is inaccurate.

Study-note section NET16

IP supplies connectionless best-effort packet delivery, not end-to-end ordering or retransmission. IPv4 addresses are 32 bits. Its minimum header is 20 bytes and can grow to 60 bytes; it is not a 32-bit header. IHL counts 32-bit words; total length includes header and payload. TTL limits lifetime across routers; the protocol field identifies TCP, UDP or another upper-layer protocol.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 28 | lines 32-45

Application Layer
The application layer in TCP/IP is equivalent to the combined session, presentation, and application layers in the OSI model and many protocols are defined at this layer.
The Process/Application Layer Protocols
• Telnet
• File Transfer Protocol (FTP)
• Network File System (NFS).
• Simple Mail Transfer Protocol (SMTP
• POP3 is used to receive mail.
• Simple Network Management Protocol (SNMP)
• Domain Name Service (DNS)
• Dynamic Host Configuration Protocol (DHCP)

Data Communication and Computer Networking module | PDF page 18 | lines 27-32

Application Layer
The Application Layer is a combination of Session, Presentation & Application Layers of OSI models and defines high level protocols like File Transfer (FTP), Electronic Mail (SMTP), Virtual Terminal (TELNET), Domain Name Service (DNS), etc.

Question sources

MOE Computer Science Exit Exam · Question 6-1

MOE Computer Science Exit Exam

Computer Science Exit Exam practice collection · Question 143

Question 152 | SM0022

A university’s private LANs and WANs provide services only to its staff, students and administrators. Which term best describes this system by its access scope?

A. Local Area Network

B. Intranet

C. Wide Area Network

D. Metropolitan Area Network

Hint

Use the cited note definitions to identify the requested function or scope, then check each alternative against that same rule.

Answer B: Intranet

The relevant distinction is who can access organizational services, rather than how far the links extend. An intranet serves an organization internally, so it can include both local and wide-area components. LAN, WAN and MAN describe geographic reach and cannot replace that access-scope classification. The option identifies an intranet without assuming a particular geographic footprint.

Why each choice is right or wrong

A - Incorrect: LAN describes geographic reach of local components rather than the organizational access scope requested.

B - Correct: An intranet serves the university’s internal members across its constituent networks.

C - Incorrect: WAN describes geographic reach of some components rather than the internal-access scope requested.

D - Incorrect: MAN describes metropolitan geographic reach rather than internal organizational access.

Primary note proof

Study-note section NET02

> PAN connects personal devices, such as Bluetooth accessories. LAN covers a local building or campus; MAN spans a metropolitan region; WAN connects distant regions. Device count alone does not determine the category. The Internet is a global network of networks, commonly the largest example of a WAN.

Study-note section NET02

> An intranet serves an organization internally; an extranet exposes selected services to approved outsiders. Neither term alone specifies geographic size. A client requests a service; a server

supplies it. Peer systems may perform both roles. Dedicated servers concentrate on service workloads but can still be clients of DNS, backup or update services. A ten-user cutoff is a teaching guideline, not a technical law. Centralization simplifies administration but creates dependencies; peer networks still need security.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 22 | lines 26-44

Personal Area Network (PAN): is a network may be spanned across a given table with distances between the devices not more than few meters. The technology used to interconnect the devices could be a Bluetooth. These networks are called Personal Area Networks, since the devices interconnected in these networks are belongs to a single person.
Local Area Network (LAN): is a network that may span across a building, or across several buildings within a single organization, by using intermediate devices, like switches and/or hubs, to interconnect devices in all floors.
Metropolitan Area Network (MAN): is a network that may span across a whole city interconnecting several buildings and organizations.
Wide Area Network (WAN): is a network that may span across multiple cities, or an entire country, or an entire continent or it may even cover the whole world. For example, an Internet is one example of WAN.

Data Communication and Computer Networking module | PDF page 24 | lines 23-35

Network Architecture: based on the architecture (where do the clients get the shared resources?), networks can be categorized into three:
Client-Server Architecture: There can be one or more systems acting as Server. Other being Client, request the Server to serve requests. Servers take and process request on clients‘ behalf.
Peer-to-Peer (Point-to-point): Two systems can be connected Point-to-Point, or in other words back-to-back fashion. They both reside on same level and called peers.
There can be hybrid network which involves network architecture of both the above types.

Question sources

MOE Computer Science Exit Exam · Question 6-2

National Computer Science Exit Exam · Question 78

National Computer Science Exit Exam

MOE Computer Science Exit Exam

Computer Science Exit Exam practice collection · Question 144

Question 153 | SM0025

At which layer of the OSI model are devices such as bridges, switches and Network Interface Cards used?

A. Physical layer

B. Application layer

C. Network layer

D. Data link layer

Hint

Match the requested scope or data unit to the layer duties in the note; distinguish hop delivery from end-to-end process delivery.

Answer D: Data-link forwarding functions, with NICs also implementing PHY

Bridges and ordinary switches inspect MAC frames at layer 2. A NIC commonly implements both physical and data-link functions, as NET09 explains; listing NICs here does not force all NIC work into one layer. D is the common frame/addressing layer for the listed devices' relevant network-interface forwarding functions.

Why each choice is right or wrong

A - Incorrect: A NIC has physical functions, but bridges/switches make layer-2 forwarding decisions beyond signal repetition.

B - Incorrect: These devices' MAC/frame operations are below application-service semantics.

C - Incorrect: Ordinary bridges and Ethernet switches do not route IP prefixes as their defining function.

D - Correct: Bridges/switches operate at layer 2, and NICs also implement link-layer MAC/frame functions.

Primary note proof

Study-note section NET09

> A NIC supplies a computer's network interface and commonly implements both physical and link functions. Calling a NIC a physical interface does not mean all its functions are layer 1. Physical specifications include connectors, signaling, voltage, timing and physical coding/modulation; the PHY interface to MAC handles hardware signaling.

Study-note section NET10

A bridge or ordinary Ethernet switch operates at layer 2. It learns source-MAC-to-port mappings, looks up the destination, forwards a known unicast to its port, filters it if the destination is on the incoming segment, and floods an unknown unicast or broadcast within its VLAN. A switch does not always send only to one destination port. Wireless access points normally bridge wireless and wired link-layer traffic.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 12 | lines 27-37

SWITCH: A switch filters and forwards data packets
across anetwork.
Unlike a hub which simply replicates what it receives on
oneport onto all the other ports, a switch keeps a record
of the MAC addresses of the devices attached to it.
When the switch receives a data packet, it forwards the
packetdirectly to the recipient device by looking up the
MAC address.
• Switch is intelligent and expensive than Hub
• Switch is a point to point communication device
• Hub is a broadcasting device

Data Communication and Computer Networking module | PDF page 12 | lines 60-61

BRIDGE: Connects two LANS having the same protocol -
(e.g. Ethernet or Token ring).

Data Communication and Computer Networking module | PDF page 17 | lines 44-53

ARP - Address Resolution Protocol: It is used to
resolve thephysical address of a device on a network,
where its logical address is known.
Physical address is the 48 bit address that is imprinted
on theNIC or LAN card, Logical address is the Internet
Address orcommonly known as IP address that is used
to uniquely & universally identify a device.
RARP- Reverse Address Resolution Protocol: It is
used bya device on the network to find its Internet
address when it knows its physical address.

Data Communication and Computer Networking module | PDF page 15 | lines 13-40

Data Link Layer
• The Data Link layer adds reliability to the physical
layer by providing error detection and correction
mechanisms.
• Framing: the Data Link layer receives the data
from Network Layer and divides the stream of bits
into fixed size manageable units called as Frames
and sends it to the physical layer. On the receiver

side, the data link layer receives the stream of bits from the physical layer and regroups them into frames and sends them to the Network layer.
• Physical Addressing: The Data link layer appends the physical address in the header of the frame before sending it to physical layer.
• Flow control: The data link layer makes sure that the sender sends the data at a speed at which the receiver canreceive it else if there is an overflow at the receiver sidethe data will be lost.
• Error Control: The data link layer imposes error control mechanism to identify lost or damaged frames, duplicateframes and then retransmit them.
• Access Control: The data link layer imposes access control mechanism to determine which device has right to send data in an multipoint connection setting.
• Main Responsibility: The main responsibility of the data link layer is hop to hop transmission of frames.

Question sources

MOE Computer Science Exit Exam · Question 7-2

National Computer Science Exit Exam · Question 39

National Computer Science Exit Exam

MOE Computer Science Exit Exam

Computer Science Exit Exam practice collection · Question 145

Question 154 | SM0035

Which listed device is an end resource used by clients, rather than an intermediary that forwards, bridges or repeats network traffic?

A. Routers

B. Network printer

C. Wireless access point

D. Hubs

Hint

Use the cited note definitions to identify the requested function or scope, then check each alternative against that same rule.

Answer B: Network printer

A network printer is an endpoint resource that receives client jobs. A router forwards packets between networks, a wireless access point normally bridges wireless and wired link traffic, and a hub repeats physical signals among ports. These are intermediary roles in the comparison. The question classifies their normal function rather than claiming that an intermediary cannot also expose a management endpoint.

Why each choice is right or wrong

A - Incorrect: Routers forward traffic between networks and are intermediaries.

B - Correct: A network printer is the client-facing end resource.

C - Incorrect: A wireless access point normally bridges wireless and wired link traffic.

D - Incorrect: A hub repeats signals between attached devices and is an intermediary.

Primary note proof

Study-note section NET09

> A repeater regenerates layer-1 signals without inspecting destination addresses. An active hub is a multiport repeater: it repeats incoming signals onto other ports, placing half-duplex endpoints in one collision domain. A passive hub is a connector. A hub neither learns MAC addresses nor eliminates collisions. An endpoint such as a network printer consumes services; routers, hubs and access points are intermediary devices.

Study-note section NET10

> A bridge or ordinary Ethernet switch operates at layer 2. It learns source-MAC-to-port mappings, looks up the destination, forwards a known unicast to its port, filters it if the destination is on the incoming segment, and floods an unknown unicast or broadcast within its VLAN. A switch does not always send only to one destination port. Wireless access points normally bridge wireless and wired link-layer traffic.

Study-note section NET-S04

> A computer network connects computers or other devices so they can exchange information and share resources such as files, storage and printers. The interconnection uses both hardware and software; neither hardware alone nor software alone is the definition of the whole network.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 12 | lines 38-52

> ROUTER: Router is a specialized network device
> used tointerconnect different types of network that
> uses different protocol.
> Router allows the users to connect several LAN and WAN
> • A LAN to another LAN
> • A WAN to another WAN
> • A LAN to the Internet

Routers use the routing table to determine how to forwardpackets.
• The list of routing tables provides directions to transfer the data to a particular network destination -various paths to forward the data.
• A router analyzes a destination IP address of a givenpacket and compares it with the routing table to decide the packet's next best path

Data Communication and Computer Networking module | PDF page 12 | lines 17-26

Active Hubs
An active hub is actually a multipart repeater. It is normallyused to create connections between stations in a physical startopology.
HUB: Hubs are commonly used to connect segments (devices)of a LAN. Hubs don‘t filter information; instead broadcast incoming packets to all computers connected to it. A hub contains multiple ports which support 8, 12 or 24 RJ-45 ports. Two types: Passive hub and Active hub. It is used in star or ring topology.

Data Communication and Computer Networking module | PDF page 22 | lines 26-44

Personal Area Network (PAN): is a network may be spanned across a given table with distances between the devices not more than few meters. The technology used to interconnect the devices could be a Bluetooth. These networks are called Personal Area Networks, since the devices interconnected in these networks are belongs to a single person.
Local Area Network (LAN): is a network that may span across a building, or across several buildings within a single organization, by using intermediate devices, like switches and/or hubs, to interconnect devices in all floors.
Metropolitan Area Network (MAN): is a network that may span across a whole city interconnecting several buildings and organizations.
Wide Area Network (WAN): is a network that may span across multiple cities, or an entire country, or an entire continent or it may even cover the whole world. For example, an Internet is one example of WAN.

Data Communication and Computer Networking module | PDF page 22 | lines 2-19

A network can be defined as two or more computers connected together in such a way that they can share resources. The primary purpose of a network is to share

resources, and a resource could be:
• a file,
• a folder,
• a printer,
• a disk drive, or just about anything else that exists on a computer.
Therefore, a computer network is simply a collection of computers or other hardware devices that are connected together, either physically or logically, using special hardware and software, to allow them to exchange information and cooperate. Networking is the term that describes the processes involved in designing, implementing, upgrading, managing and otherwise working with networks and network technologies.

Question sources

MOE Computer Science Exit Exam · Question 11-1

National Computer Science Exit Exam · Question 15

National Computer Science Exit Exam

MOE Computer Science Exit Exam

Computer Science Exit Exam practice collection · Question 146

Question 155 | SM0036

_____ is a network architecture characteristic that states a network can expand quickly to address needs of new users and applications without having impact on the services delivered to existing users.

A. Security

B. Quality of service

C. Fault tolerance

D. Scalability

Hint

Use the cited note definitions to identify the requested function or scope, then check each alternative against that same rule.

Answer D: Scalability

Scalability is explicitly continued predictable function as system size grows, matching expansion without undermining existing service. Evidence: PDF 32.

Why each choice is right or wrong

A - Incorrect: Security concerns authorized access, not size growth (PDF 32.)

B - Incorrect: Quality of service is not the named growth principle (PDF 32.)

C - Incorrect: Fault tolerance is continued operation through failures rather than growth (PDF 32.)

D - Correct: Scalability is the explicit size-growth principle (PDF 32.)

Primary note proof

Study-note section NET01

> Delivery means reaching the intended recipient; accuracy means preserving content; timeliness means meeting a deadline; jitter means variation in arrival delay. A call can have acceptable average delay yet sound broken because of jitter. Throughput measures achieved transfer rate, reliability measures dependable operation, and security concerns unauthorized actions. Scalability means accommodating growth without unacceptable service degradation.

Study-note section NET-S02

> Quality of service (QoS) controls traffic treatment to meet objectives such as throughput, delay, jitter or loss. Classification, queue scheduling and allocation of buffer or bandwidth resources implement such treatment. QoS concerns delivered service behavior; scalability concerns accommodating growth, and security concerns unauthorized actions.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 32 | lines 2-5

> Scalable systems are those that grow in
> accordance with policy; i.e. they continue to
> function predictably, even as they increase in
> size.

Question sources

MOE Computer Science Exit Exam · Question 11-2

National Computer Science Exit Exam · Question 17

National Computer Science Exit Exam · Question 19

National Computer Science Exit Exam

MOE Computer Science Exit Exam

Computer Science Exit Exam practice collection · Question 147

Question 156 | SM0038

Which network type is the largest as compared to the rest?

A. Wide Area Network

B. Metropolitan Area Network

C. The Internet

D. Local Area Network

Hint

Use the cited note definitions to identify the requested function or scope, then check each alternative against that same rule.

Answer C: The Internet

The Internet names the particular global network of networks, while WAN, MAN and LAN name scope categories. NET02 explicitly gives the Internet as the largest common WAN example. Thus C is the intended largest actual network in the comparison, even though WAN includes Internet-scale networks rather than being a disjoint smaller category.

Why each choice is right or wrong

A - Incorrect: WAN is a category that includes the Internet, not a separate specific network shown to be larger.

B - Incorrect: MAN spans a metropolitan area rather than the global network of networks.

C - Correct: NET02 identifies the global Internet as the largest common WAN example.

D - Incorrect: LAN covers a local building/campus and is much narrower in geographic scope.

Primary note proof

Study-note section NET02

> PAN connects personal devices, such as Bluetooth accessories. LAN covers a local building or campus; MAN spans a metropolitan region; WAN connects distant regions. Device count alone does not determine the category. The Internet is a global network of networks, commonly the largest example of a WAN.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 22 | lines 26-44

> Personal Area Network (PAN): is a network may be spanned across a given table with distances between the devices not more than few meters. The technology used to interconnect the devices could be a Bluetooth. These networks are called Personal Area Networks, since the devices interconnected in these networks are belongs to a single person.

Local Area Network (LAN): is a network that may span across a building, or across several buildings within a single organization, by using intermediate devices, like switches and/or hubs, to interconnect devices in all floors.
Metropolitan Area Network (MAN): is a network that may span across a whole city interconnecting several buildings and organizations.
Wide Area Network (WAN): is a network that may span across multiple cities, or an entire country, or an entire continent or it may even cover the whole world. For example, an Internet is one example of WAN.

Question sources

MOE Computer Science Exit Exam · Question 11-4

National Computer Science Exit Exam · Question 88

National Computer Science Exit Exam

Computer Science Exit Exam practice collection · Question 148

Question 157 | SM0057

Which statement is incorrect when packet switching means connectionless datagram switching?

A. In packet switching, messages are sent in small blocks

B. In packet switching, an end-to-end connection has to be established

C. In circuit switching, a channel is dedicatedly used

D. For bursty traffic, statistical packet sharing can use capacity that dedicated circuits would reserve while idle.

Hint

Compare signal repetition, frame forwarding, packet routing and policy enforcement using the stated device or traffic assumptions.

Answer B: In packet switching, an end-to-end connection has to be established

Datagram switching divides messages into packets and forwards those packets independently without requiring end-to-end connection establishment. Circuit switching reserves resources along a path. Statistical sharing lets bursty packet traffic use capacity that would otherwise remain reserved but idle; this is a conditional utilization advantage, not a universal claim that packets outperform circuits for every workload or metric.

Why each choice is right or wrong

A - Incorrect: Packet switching divides messages into smaller packets.

B - Correct: Connectionless datagrams do not require end-to-end connection setup.

C - Incorrect: Circuit switching reserves channel resources for the connection.

D - Incorrect: For bursty traffic, shared packet links can avoid idle dedicated reservations; the qualified statement is true.

Primary note proof

Study-note section NET31

Circuit switching sets up a path with reserved resources, transfers data, then releases it. Predictable allocated bandwidth trades against setup/blocking and wasted reservation during silence. A traditional telephone call is the standard example. Packet switching divides data into packets that share links statistically; queueing can add variable delay and loss. This does not make modern voice-over-packet impossible: buffering, scheduling and capacity planning manage it.

Study-note section NET31

Datagram packets are forwarded independently. Virtual circuits establish forwarding state, but resource reservation is optional, not a necessary property of every virtual circuit. Message switching stores a complete message before forwarding, without a dedicated end-to-end path. Packet store-and-forward waits for the full packet/frame; cut-through starts after enough header arrives; fragment-free historically waits through the initial collision-sensitive portion. No routing algorithm guarantees that every packet always takes the geometrically shortest route.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 20 | lines 12-26

Circuit Switching: In circuit switching, two communicating stations are connected by a dedicated communication path which consists of intermediate nodes in the network and the links that connect these nodes.
It involved the following three distinct steps
• Circuit Establishment: To establish an end-to-end connection before any transfer of data.
• Data transfer: Transfer data is from the source to the destination. The data may be analog or digital, depending on the nature of the network. The connection is generally full-duplex.
• Circuit disconnect: Terminate connection at the end of data transfer. Signals must be propagated to deallocate the dedicated resources.

Data Communication and Computer Networking module | PDF page 20 | lines 27-36

Message Switching:
Packet Switching: Packet switching was designed to

address the shortcomings of circuit switching in dealing with data communication. Unlike circuit switching where communication is continuous along a dedicated circuit, in packet switching, communication is discrete in form of packets.
The three switching modes to choose from are:
• Cut-through
• Store-and-forward
• Fragment-free

Data Communication and Computer Networking module | PDF page 15 | lines 41-61

Network Layer
• The network layer makes sure that the data is deliveredto the receiver despite multiple intermediate devices.
• The network layer at the sending side accepts data from the transport layer, divides it into packets, addsaddressing information in the header and passes it tothe data link layer.
• The network layer is responsible for source todestination of delivery of data.
• The network layer uses logical address commonlyknown as IP address to recognize devices on the network.
• Each packet is independent of the other and may travelusing different routes to reach the receiver hence may arrive out of turn at the receiver (Routing).
• The Network layer does not perform any flow controlor error control
• The main responsibility of Network Layer is transmission of packets from source to destination

Question sources

MOE Computer Science Exit Exam · Question 16-4

National Computer Science Exit Exam · Question 97

National Computer Science Exit Exam

MOE Computer Science Exit Exam

Computer Science Exit Exam practice collection · Question 149

Question 158 | SM0062

Which layer uses port number to identify applications?

A. Transport layer

B. Physical layer

C. Network layer

D. Application layer

Hint

Match the requested scope or data unit to the layer duties in the note; distinguish hop delivery from end-to-end process delivery.

Answer A: Transport layer

Ports explicitly identify source and destination processes for transport delivery. Evidence: PDF 16, 28, 14, 15, 16.

Why each choice is right or wrong

A - Correct: Transport uses port addresses for processes (PDF 16, 28, 14, 15, 16.)

B - Incorrect: Physical represents bits and signals (PDF 16, 28, 14, 15, 16.)

C - Incorrect: Network uses logical IP addresses (PDF 16, 28, 14, 15, 16.)

D - Incorrect: Application uses transport services but port addressing is assigned to transport (PDF 16, 28, 14, 15, 16.)

Primary note proof

Study-note section NET17

> Ports identify transport endpoints; the application can choose a transport and request socket buffer sizes, subject to OS limits. A TCP connection is identified by source/destination IP and source/destination port, with TCP understood. IPv4 protocol numbers identify upper protocols; 80 is a usual HTTP port, not an IP protocol number. Clients often use ephemeral ports. SCTP is a reliable message-oriented transport with multiple streams.

Study-note section NET12

> Sending proceeds from application data to transport segment/datagram, network packet, link frame and physical bits/symbols; receiving reverses the order. Each layer serves the layer above. A router removes a received link frame, inspects IP, and creates a new link frame for the next hop. MAC addresses usually change across routed hops; end-to-end IP addresses ordinarily remain until translation.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 16 | lines 2-17

• At the sending side, the transport layer receives data from the session layer, divides it into units called segments and sends it to the network layer.
• To ensure process to process delivery the transport layer makes use of port address to identify the data from the sending and receiving process.
• The data can be transported in a connection oriented or connectionless manner.
• The Transport layer is responsible for segmentation and reassembly of the message into segments which bear sequence numbers.
• The transport layer also carries out flow control and error control functions; but unlike data link layer these are end to end rather than node to node.
• The main responsibility of the transport layer is process to process delivery of the entire message

Data Communication and Computer Networking module | PDF page 28 | lines 2-14

TCP and UDP must use port numbers to communicate with the upper layers, because they‘re what keep track of different conversations crossing the network simultaneously. These port numbers identify the source and destination application or process in the TCP segment. There are 216 = 65,536 ports available.
Well-known ports: The port numbers range from 0 to 1,023.
Registered ports: The port numbers range from 1,024 to 49,151. Registered ports are used by applications or services that need to have consistent port assignments.
Dynamic or private ports: The port numbers range from 49,152 to 65,535.

Data Communication and Computer Networking module | PDF page 14 | lines 32-49

Physical Layer:
• The Physical Layer provides a standardized interface to physical transmission media, including: Mechanical specification of electrical connectors and cables, for example maximum cable length, Electrical specification of transmission line and Bit-by-bit or symbol-by-symbol delivery.
• Interface: The Physical Layer defines the characteristics of interfaces between the devices & transmission medium.
• Representation of bits: The physical layer is concerned with transmission of signals from one device to another which involves converting data (1_s & 0_s) into signals and vice versa. It is not concerned with the meaning or interpretation of bits.

• Data rate: The physical layer defines the data transmission rate i.e. number of bits sent per second. It is the responsibility of the physical layer to maintain the defined data rate.

Data Communication and Computer Networking module | PDF page 15 | lines 41-61

Network Layer
• The network layer makes sure that the data is deliveredto the receiver despite multiple intermediate devices.
• The network layer at the sending side accepts data from the transport layer, divides it into packets, addsaddressing information in the header and passes it tothe data link layer.
• The network layer is responsible for source todestination of delivery of data.
• The network layer uses logical address commonlyknown as IP address to recognize devices on the network.
• Each packet is independent of the other and may travelusing different routes to reach the receiver hence may arrive out of turn at the receiver (Routing).
• The Network layer does not perform any flow controlor error control
• The main responsibility of Network Layer is transmission of packets from source to destination

Data Communication and Computer Networking module | PDF page 16 | lines 43-47

Application Layer
• The application layer enables the user to communicate its data to the receiver by providing certain services.
• The main Responsibility of Application layer is to provide the user access to network resources.

Question sources

MOE Computer Science Exit Exam · Question 18-1

Computer Science Exit Exam practice collection · Question 150

Question 159 | SM0225

In which network topology does a single line cable called a backbone connect all nodes on a network without intervening connected devices?

A. Bus

B. Ring

C. Star

D. Mesh

Hint

Draw the links and identify shared components, alternate paths and the effect of the specified failure or growth requirement.

Answer A: Bus

Bus explicitly connects all devices to a central backbone cable terminated at both ends. Evidence: PDF 23, 23, 23, 23.

Why each choice is right or wrong

A - Correct: Bus has the stated shared backbone (PDF 23, 23, 23, 23.)

B - Incorrect: Ring is a closed neighbor loop (PDF 23, 23, 23, 23.)

C - Incorrect: Star uses a central hub/switch and separate links (PDF 23, 23, 23, 23.)

D - Incorrect: Mesh has many direct node-pair links (PDF 23, 23, 23, 23.)

Primary note proof

Study-note section NET08

> Bus uses a shared backbone; an unterminated break can disrupt the segment. Star connects endpoints through a central device: one edge failure isolates that endpoint, whereas central failure affects the star. Ring forms a loop; basic single rings are vulnerable to a break, while protected dual rings differ. Token passing is associated with Token Ring but is an access method, not a necessary property of every ring. Tree is hierarchical; hybrid combines arrangements.

Study-note section NET08

> Physical topology describes link layout; logical topology describes communication/access relationships. Point-to-point links join two endpoints; multipoint links share a medium. A full mesh consists of point-to-point links.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 23 | lines 4-18

> Bus Topology: in this topology all devices are
> connected to a central cable, called the bus or
> backbone, which is terminated at its ends. The

purpose of the terminators is to stop the signal from bouncing, thereby clearing the cable so that other computers can send data. Message transmitted along the Bus is visible to all computers connected to the backbone cable. As the message arrives at each workstation, the workstation checks the destination address contained in the message either to process or drop the packet if it matches or not respectively. Its advantages are, ease of installation and less amount of cable requirement. Its main drawback is, the entire network will be shut down if there is a break in the main cable.

Data Communication and Computer Networking module | PDF page 23 | lines 19-34

Star Topology: in this topology, each node is connected directly to a central device called a hub or a switch. Data on a star network passes through the central device (switch) before continuing to its destination. The central device manages and controls all functions of the network. This configuration is common with twisted pair cable. RJ-45 Connectors are used to connect the cable to the Network Interface Card (NIC) of each computer. Its advantages include, ease of installation and reconfiguration, robust (ease of fault identification and isolation), link failure only affects device(s) connected to that link, and is less expensive than mesh. Its drawbacks include more cable requirements (than bus and ring) and single point of failure (if central device fail, the whole system will be down).

Data Communication and Computer Networking module | PDF page 23 | lines 35-44

Ring Topology: in this topology, all devices are connected to one another in the shape of a closed loop, so that each device is connected directly to two other devices, one on either side of it. Some of its advantages include, easy to install and reconfigure, less expensive (than mesh), and performance is even despite the number of users. Its cons include, break in the ring (such as a disabled station) can disable the entire network, and limitations on media and traffic (limitation on ring length and number of devices).

Data Communication and Computer Networking module | PDF page 23 | lines 45-53

Mesh Topology: in this topology devices are connected with many redundant interconnections

between network nodes. In a full mesh topology, every node has a connection to every other node in the network, which makes it the most expensive topology over all the other topologies. The number of cables grows fast as the number of nodes increases, and it can be calculated by using the general formula ((n (n - 1)) /2), where n is the number of nodes in the

Question sources

Computer Science Exit Exam · Sene 2016 · Question 8-3

Computer Science Exit Exam practice collection · Question 158

Question 160 | SM0233

In computer networking, _____ refers to how various nodes, devices, and connections on your network are physically or logically arranged in relation to each other.

A. Network layer

B. Network installation

C. Network protocol

D. Network topology

Hint

Compare signal repetition, frame forwarding, packet routing and policy enforcement using the stated device or traffic assumptions.

Answer D: Network topology

Network topology is the shape/layout and geometrical relation of links and devices, including physical and logical connectedness. Evidence: PDF 22, 5.

Why each choice is right or wrong

A - Incorrect: Network layer is a protocol responsibility layer (PDF 22, 5.)

B - Incorrect: Installation is the activity of building, not the layout name (PDF 22, 5.)

C - Incorrect: Protocol is a communication rule set (PDF 22, 5.)

D - Correct: Topology is exactly the arrangement concept (PDF 22, 5.)

Primary note proof

Study-note section NET08

Physical topology describes link layout; logical topology describes communication/access relationships. Point-to-point links join two endpoints; multipoint links share a medium. A full mesh consists of point-to-point links.

Study-note section NET03

Protocol syntax defines message structure, semantics defines field meanings, and timing defines when/how fast exchanges occur. A standard supports interoperability. De facto means established through use; de jure means formally approved. ISO develops international standards; IEEE develops LAN standards such as 802.3 and 802.11; ITU-T develops telecommunications standards. ANSI coordinates US standards, EIA is associated with interface standards, and FCC is a regulator.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 22 | lines 45-52

Inter-connectivity: components of a network,
including end devices and interconnecting devices,
can be connected to each other differently in some
fashion. By connectedness we mean either logically,
physically or both ways. Network topology refers to
the shape of a network, or the network‘s layout. It is
the geometric representation of the relationship of all
the links and linking devices to one another. There are

Data Communication and Computer Networking module | PDF page 5 | lines 70-81

PROTOCOL
Protocol can be defined as set of rules that governs data
communications.
It defines what is to be communicated, how it is to be
communicated and when it is to be communicated.
There are three key elements of a protocol:
Syntax: It means the structure or format of the data. It is the
arrangement of data in a particular order.
Semantics: It tells the meaning of each section of bits and
indicates the interpretation of each section.
Timing: It tells the sender about the readiness of the receiver to
receive the data

Question sources

Computer Science Exit Exam · Sene 2016 · Question 11-1

Computer Science Exit Exam practice collection · Question 163

Question 161 | SM0264

Which one of the following IS NOT a component of communication?

A. Distance

B. Source

C. Destination

D. Medium

Hint

Use the cited note definitions to identify the requested function or scope, then check each alternative against that same rule.

Answer A: Distance

The five components are message, sender, receiver, medium and protocol. Distance is a property of a path, not a component in this definition. Evidence: PDF 5.

Why each choice is right or wrong

A - Correct: Distance is not one of the five defined components (PDF 5.)

B - Incorrect: Source corresponds to sender (PDF 5.)

C - Incorrect: Destination corresponds to receiver (PDF 5.)

D - Incorrect: Medium is explicitly listed (PDF 5.)

Primary note proof

Study-note section NET01

> Data are raw representations; information is data interpreted for a purpose. Communication requires a message, sender, receiver, medium and agreed protocol. A source creates data; a transmitter converts it to a signal; a receiver reconstructs data. Distance affects engineering but is not a sixth component.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 5 | lines 23-35

> A Data Communication system has five components:-
> • Message:- is the information to be communicated by the sender to the receiver.
> • Sender The sender is any device that is capable of sending the data (message).
> • Receiver: - is a device that the sender wants to communicate the data (message).
> • Transmission Medium: - It is the path by which the message travels from sender to receiver. It can be wired or wireless and many subtypes in both.

• Protocol:- It is an agreed upon set or rules used by the sender and receiver to communicate data. Rules that govern data communication.

Question sources

Computer Science Exit Exam · Sene 2016 · Question 21-1

Computer Science Exit Exam practice collection · Question 162

Question 162 | SM0274

In which network topology should every computer have N-1 I/O ports when there are N computers in the network?

A. Star

B. Mesh

C. Bus

D. Ring

Hint

Draw the links and identify shared components, alternate paths and the effect of the specified failure or growth requirement.

Answer B: Mesh

In full mesh every node directly connects to each of the other N-1 nodes. With a separate port for each dedicated link, each computer needs N-1 ports. Evidence: PDF 23, 23, 23, 23.

Why each choice is right or wrong

A - Incorrect: Star needs one link per end device to the center (PDF 23, 23, 23, 23.)

B - Correct: Full mesh has one connection to each other node (PDF 23, 23, 23, 23.)

C - Incorrect: Bus shares a backbone rather than N-1 separate links (PDF 23, 23, 23, 23.)

D - Incorrect: Ring connects each node to two neighbors (PDF 23, 23, 23, 23.)

Primary note proof

Study-note section NET08

A full undirected mesh of n nodes needs n(n-1)/2 links and n-1 interfaces per node. For 50 nodes: 50×49/2=1225 links. Redundant paths improve fault tolerance at greater cable and interface cost.

Study-note section NET08

Bus uses a shared backbone; an unterminated break can disrupt the segment. Star connects endpoints through a central device: one edge failure isolates that endpoint, whereas central failure affects the star. Ring forms a loop; basic single rings are vulnerable to a break, while

protected dual rings differ. Token passing is associated with Token Ring but is an access method, not a necessary property of every ring. Tree is hierarchical; hybrid combines arrangements.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 23 | lines 45-53

Mesh Topology: in this topology devices are connected with many redundant interconnections between network nodes. In a full mesh topology, every node has a connection to every other node in the network, which makes it the most expensive topology over all the other topologies. The number of cables grows fast as the number of nodes increases, and it can be calculated by using the general formula ((n (n - 1)) /2), where n is the number of nodes in the

Data Communication and Computer Networking module | PDF page 23 | lines 19-34

Star Topology: in this topology, each node is connected directly to a central device called a hub or a switch. Data on a star network passes through the central device (switch) before continuing to its destination. The central device manages and controls all functions of the network. This configuration is common with twisted pair cable. RJ-45 Connectors are used to connect the cable to the Network Interface Card (NIC) of each computer. Its advantages include, ease of installation and reconfiguration, robust (ease of fault identification and isolation), link failure only affects device(s) connected to that link, and is less expensive than mesh. Its drawbacks include more cable requirements (than bus and ring) and single point of failure (if central device fail, the whole system will be down).

Data Communication and Computer Networking module | PDF page 23 | lines 35-44

Ring Topology: in this topology, all devices are connected to one another in the shape of a closed loop, so that each device is connected directly to two other devices, one on either side of it. Some of its advantages include, easy to install and reconfigure, less expensive (than mesh), and performance is even despite the number of users. Its cons include, break in the ring (such as a disabled station) can disable the entire network, and limitations on media and traffic (limitation on ring length and number of devices).

Data Communication and Computer Networking module | PDF page 23 | lines 4-18

> Bus Topology: in this topology all devices are connected to a central cable, called the bus or backbone, which is terminated at its ends. The purpose of the terminators is to stop the signal from bouncing, thereby clearing the cable so that other computers can send data. Message transmitted along the Bus is visible to all computers connected to the backbone cable. As the message arrives at each workstation, the workstation checks the destination address contained in the message either to process or drop the packet if it matches or not respectively. Its advantages are, ease of installation and less amount of cable requirement. Its main drawback is, the entire network will be shut down if there is a break in the main cable.

Question sources

Computer Science Exit Exam · Sene 2016 · Question 24-2

Computer Science Exit Exam practice collection · Question 159

Question 163 | SM0291

In data communication, data rate refers how fast we can send data and is measured in bits per second. Which one of
the following is not a factor for data rate?

A. Travel distance

B. Levels of the signals

[SS

C. Bandwidth available

D. Level of noise

Hint

Use the cited note definitions to identify the requested function or scope, then check each alternative against that same rule.

Answer A: Travel distance is not an explicit channel-capacity formula variable

NET05 gives Nyquist in terms of bandwidth and signal states, and Shannon in terms of bandwidth and signal-to-noise ratio. Distance is not an independent variable in those simplified capacity formulas, so A is the intended comparison. It can still affect practical achievable rate through attenuation and delay. The image confirms travel distance despite noise in another extracted option.

Why each choice is right or wrong

A - Correct: Distance is absent as an independent variable in the simplified formulas, although it affects real links indirectly.

B - Incorrect: The number of signal levels appears explicitly in Nyquist through log2(M).

C - Incorrect: Available bandwidth directly appears as B in both Nyquist and Shannon capacity expressions.

D - Incorrect: Noise affects signal-to-noise ratio and therefore the Shannon capacity limit.

Primary note proof

Study-note section NET05

For an ideal noiseless channel, Nyquist gives R≤2B log2(M). For Gaussian noise, Shannon gives C=B log2(1+S/N), with a linear power ratio; SNR(dB)=10 log10(S/N). Bandwidth, signal levels and noise appear explicitly. Distance affects attenuation, delay and often achievable rate, but is not a separate variable in these simplified capacity formulas.

Study-note section NET06

Transmission delay is packet bits divided by link bit rate; propagation delay is distance divided by signal speed. Processing and queueing add delay. A 1000-byte packet takes 0.8 ms to serialize at 10 Mbit/s; increasing line rate does not reduce propagation time.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 9 | lines 2-14

BIT LENGTH or Bit Interval (Tb)
It is the time required to send one bit.
It is measured in seconds.
BIT RATE
It is the number of bits transmitted in one second.
It is expressed as bits per second (bps).
Relation between bit rate and bit interval can be as follows
Bit rate = 1 / Bit interval
Baud Rate
It is the rate of Signal Speed, i.e the rate at which the signal
changes.
A digital signal with two levels 0_& 1_will have the same
baud rate and bit rate & bit rate.

Data Communication and Computer Networking module | PDF page 10 | lines 18-35

receiver.There are three causes of impairment:
• Attenuation
• Distortion
• Noise
Attenuation
Attenuation results in loss of energy due to distance.

Whena signal travels through a medium, it loses some of its energy in overcoming the resistance of the medium. The electrical energy in the signal may convert to heat. To compensate for this loss, amplifiers are used to amplify thesignal.
Distortion
Distortion changes the shape of the signal.
Noise
Noise is any unwanted signal that is mixed or combined with the original signal during transmission. Due to noise the original signal is altered and signal received is not sameas the one sent.

Data Communication and Computer Networking module | PDF page 9 | lines 29-49

Transmission of Digital signal: Digital signal can be transmitted in the following two ways:
• Baseband Transmission: The signal is transmitted without making any change to it (i.e. Without modulation)
o In baseband transmission, the bandwidth of the signal to be transmitted has to be less than the bandwidth of the channel.
o Ex. Consider a Baseband channel with lower frequency 0Hz and higher frequency 100Hz, hence its bandwidth is 100 (Bandwidth is calculated by getting the difference between the highest and lowest frequency)
o A channel whose bandwidth is more than the bandwidth of the signal is called Wideband channel
o A channel whose bandwidth is less than the bandwidth of the signal is called Narrowband channel
• Broadband Transmission: Given a bandpass channel, a digital signal cannot be transmitted directly through it
o In broadband transmission we use modulation, i.e. we change the signal to analog signal before transmitting it.

Question sources

Computer Science Exit Exam · Sene 2016 · Question 30-1

Question 164 | SM0292

Which layer of the OSI model ensures that the whole message (group of packets) arrives at the destination intact and in order?

A. Session layer

B. Transport layer

C. Data link layer

D. Network layer

Hint

Match the requested scope or data unit to the layer duties in the note; distinguish hop delivery from end-to-end process delivery.

Answer B: Transport layer

Transport explicitly makes process-delivered data intact and ordered, using sequence-numbered segments and end-to-end error control. Evidence: PDF 16, 15, 15, 16.

Why each choice is right or wrong

A - Incorrect: Session controls dialogs/checkpoints (PDF 16, 15, 15, 16.)

B - Correct: Transport explicitly ensures intact and ordered whole-message delivery (PDF 16, 15, 15, 16.)

C - Incorrect: Data link controls hop-to-hop frames rather than the entire end-to-end message (PDF 16, 15, 15, 16.)

D - Incorrect: Network packets can arrive out of order (PDF 16, 15, 15, 16.)

Primary note proof

Study-note section NET17

> TCP offers a reliable ordered byte stream using sequence numbers, acknowledgments, retransmission and windows. Flow control protects the receiver; congestion control protects network capacity. UDP sends independent datagrams with ports and a checksum but no built-in setup, delivery guarantee, retransmission or ordering. Live interactive traffic may choose UDP when late data is less useful than lost data. Application protocols can add reliability over UDP.

Study-note section NET14

> Controlled access uses polling, reservations or a token to grant turns; correctly coordinated access avoids contention collisions. Channelization divides frequency, time or code resources. Stop-and-wait sends one frame and waits for ACK, retransmitting on timeout; sequence bits distinguish duplicates. Sliding windows permit multiple unacknowledged frames. Link reliability/flow control is hop-local; transport reliability/flow control is end-to-end. Ethernet detects corruption but does not itself guarantee reliable delivery.

Study-note section NET19

OSI session roles establish/manage dialogs and can coordinate checkpoints so transfer resumes after interruption. Presentation roles translate encodings and handle compression/encryption. Compression reduces representation size; encryption hides content and need not shrink it. Application protocols provide services directly to applications. Practical implementations distribute these functions differently; TLS is not proof of a separate physical presentation-layer device.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 16 | lines 2-17

• At the sending side, the transport layer receives data from the session layer, divides it into units called segments and sends it to the network layer.
• To ensure process to process delivery the transport layer makes use of port address to identify the data from the sending and receiving process.
• The data can be transported in a connection oriented or connectionless manner.
• The Transport layer is responsible for segmentation and reassembly of the message into segments which bear sequence numbers.
• The transport layer also carries out flow control and error control functions; but unlike data link layer these are end to end rather than node to node.
• The main responsibility of the transport layer is process to process delivery of the entire message

Data Communication and Computer Networking module | PDF page 15 | lines 13-40

Data Link Layer
• The Data Link layer adds reliability to the physical layer by providing error detection and correction mechanisms.
• Framing: the Data Link layer receives the data from Network Layer and divides the stream of bits into fixed size manageable units called as Frames and sends it to the physical layer. On the receiver side, the data link layer receives the stream of bits from the physical layer and regroups them into frames and sends them to the Network layer.
• Physical Addressing: The Data link layer appends the physical address in the header of the frame before sending it to physical layer.
• Flow control: The data link layer makes sure that the sender sends the data at a speed at which the receiver canreceive it else if there is an overflow at the receiver sidethe data will be lost.

• Error Control: The data link layer imposes error control mechanism to identify lost or damaged frames, duplicateframes and then retransmit them.
• Access Control: The data link layer imposes access control mechanism to determine which device has right to send data in an multipoint connection setting.
• Main Responsibility: The main responsibility of the data link layer is hop to hop transmission of frames.

Data Communication and Computer Networking module | PDF page 15 | lines 41-61

Network Layer
• The network layer makes sure that the data is deliveredto the receiver despite multiple intermediate devices.
• The network layer at the sending side accepts data from the transport layer, divides it into packets, addsaddressing information in the header and passes it tothe data link layer.
• The network layer is responsible for source todestination of delivery of data.
• The network layer uses logical address commonlyknown as IP address to recognize devices on the network.
• Each packet is independent of the other and may travelusing different routes to reach the receiver hence may arrive out of turn at the receiver (Routing).
• The Network layer does not perform any flow controlor error control
• The main responsibility of Network Layer is transmission of packets from source to destination

Data Communication and Computer Networking module | PDF page 16 | lines 18-32

Session Layer
• The session layer establishes a session between the communicating devices called dialog and synchronizes their interaction. It is the responsibility of the session layer to establish and synchronize the dialogs. It is also called the network dialog controller.
• The session layer at the sending side accepts data from the presentation layer adds checkpoints to it called sync bits and passes the data to the transport layer. At the receiving end the session layer receives

data from the transport layer removes the checkpoints inserted previously and passes the data to the presentation layer. So, the main responsibility of session layer is dialog control and synchronization.

Question sources

Computer Science Exit Exam · Sene 2016 · Question 30-2

Computer Science Exit Exam practice collection · Question 165

Question 165 | SS098

Which of the following is not a valid host address within the network 172.17.128.0/21 ?

A. 172.17.128.1/21

B. 172.17.135.255 /21

C. 172.17.135.0 /21

D. 172.17.128.255/21

Hint

Convert the mask to a prefix, separate network and host bits, and apply the relevant subnet-count or usable-host rule.

Answer B: 172.17.135.255/21 is broadcast

A /21 groups eight third-octet values, here 128-135. The network is 172.17.128.0 and its broadcast is 172.17.135.255. B sets every host bit to one and cannot be assigned to an ordinary host. The other choices are inside the usable range; ending in .0 or .255 alone does not make an address reserved.

Why each choice is right or wrong

A - Incorrect: 172.17.128.1 is one above the network boundary and is a valid usable host.

B - Correct: 172.17.135.255 sets all eleven host bits to one and is the subnet broadcast address.

C - Incorrect: 172.17.135.0 is inside the /21 block; its host bits are not all zero or all one.

D - Incorrect: 172.17.128.255 is an interior host; the .255 ending alone does not make it /21 broadcast.

Primary note proof

Study-note section NET25

For ordinary broadcast LANs let h=32-p. Total addresses=2^h; usable hosts=2^h-2, reserving network and directed broadcast. Find the changing octet's increment as 256-mask octet, round the address down to a multiple, and extend through the next boundary minus one.

Study-note section NET25

192.168.2.64/26 spans .64-.127; usable .65-.126 gives 62 hosts. 192.168.10.25/28 spans .16-.31, so its network is .16. 172.17.128.0/21 spans 172.17.128.0-172.17.135.255; .128.255 and .135.0 are valid interior hosts, but .135.255 is broadcast. /27 gives 32 total and 30 usable, not 32 usable.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 18 | lines 45-54

IP addresses: IP address uniquely identifies a device on the
Internet. Every host and router on the Internet has an IP address,
which encodes its network number and host number.
• The combination is unique: in principle, no two
machines on the Internet have the same IP address.
• An IPv4 address is 32 bits long
• They are used in the Source address and Destination
address fields of IP packets.
• An IP address does not refer to a host but it refers to a
network interface.

Data Communication and Computer Networking module | PDF page 19 | lines 2-22

Address Space: An address space is the total
number ofaddresses used by the protocol.
• If a protocol uses N bits to define an address,
the address space is 2N
because each bit can
have twodifferent values (0 or 1) and N bits
can have 2N values.
• IPv4 uses 32-bit addresses, which means that
the address space is 232 or 4,294,967,296
(more than 4billion).
Notations: There are two notations to show an IPv4 address:
• Binary notation: The IPv4 address is displayed
as 32bits. ex. 11000001 10000011 00011011
11111111
• Dotted decimal notation: To make the IPv4
address easier to read, Internet addresses are
usually written in decimal form with a decimal
point (dot) separatingthe bytes. Each byte (octet)
is 8 bits hence each number in dotted-decimal
notation is a value rangingfrom 0 to 255. Ex.
129.11.11.239

Data Communication and Computer Networking module | PDF page 19 | lines 23-36

Classful addressing : In classful addressing, the
addressspace is divided into five classes: A, B, C,
D, and E.
• Netid and Hostid In classful addressing, an IP

addressin class A, B, or C is divided into netid
and hostid.
Subnetting: It allows a network to be split into several
parts for internal use but still act like a single network to
the outsideworld.
• To implement subnetting, the router needs a
subnet mask that indicates the split between
network + subnet number and host. Ex.
255.255.252.0/22. A‖/22‖ to indicate that the
subnet mask is 22 bits long.

Question sources

Computer Science model exam collection · Question 5

Question 166 | SS111

Which of the following is not the function of Cross-over UTP cable?

A. To connect router to pc

B. To connect switch to switch

C. To connect switch to pc

D. To connect pc to pc

Hint

Compare the signal mechanism, medium properties or transmission direction against the definitions and stated physical assumptions.

Answer C: Switch-to-PC normally uses straight-through cable in legacy Ethernet

Under the legacy MDI/MDI-X convention, a switch port and PC have unlike roles and use straight-through cable. PCs and router Ethernet endpoints conventionally share the endpoint role, while two switches share the switch role, so those like-role links use crossover. Auto-MDI-X can remove the practical requirement; the question is testing the conventional cable-role distinction.

Why each choice is right or wrong

A - Incorrect: A legacy router Ethernet endpoint and PC have like interface roles, so crossover is appropriate.

B - Incorrect: Two legacy switch ports have like roles and conventionally require crossover.

C - Correct: Switch and PC have unlike legacy interface roles and normally use straight-through cable.

D - Incorrect: Two PCs have like legacy interface roles; NET07 explicitly names PC-PC as a crossover example.

Primary note proof

Study-note section NET07

Radio, microwave and infrared are unguided media. Ground waves follow Earth, sky waves can reflect from ionized layers, and line-of-sight paths require suitable visibility. Microwaves are radio waves in the broader physical classification. Infrared generally does not penetrate walls. Directionality depends on antennas: omnidirectional means broad azimuth coverage, not equal radiation in every 3-D direction. Legacy Ethernet straight-through cables join unlike MDI/MDI-X roles; crossover joins like roles, such as PC-PC or switch-switch. Auto-MDI-X can remove that requirement.

Study-note section NET-S07

For legacy fixed Ethernet port roles, PCs and router Ethernet endpoints use the same endpoint role, while ordinary switch ports use the opposite role. Thus a direct router-to-PC link uses crossover wiring; PC-to-switch or router-to-switch uses straight-through wiring. Automatic MDI-X can remove the need to choose the crossover manually.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 11 | lines 23-33

Twisted-pair cable: Consists of two conductors (normally copper), each with its own plastic insulation, twisted together.
Two types
• Unshielded Twisted-Pair cable (UTP)
• Shielded Twisted-Pair cable (STP)
Coaxial cable:- uses copper wire to conduct the signals electronically
Fiber-optic cable:- uses glass or plastic conductor and transmits the signals as light
Wireless/Unguided media the signal propagates in the atmosphere and in outer space

Data Communication and Computer Networking module | PDF page 23 | lines 19-34

Star Topology: in this topology, each node is connected directly to a central device called a hub or a switch. Data on a star network passes through the central device (switch) before continuing to its destination. The central device manages and controls all functions of the network. This configuration is common with twisted pair cable. RJ-45 Connectors are used to connect the cable to the Network Interface Card (NIC) of each computer. Its advantages include, ease of installation and reconfiguration, robust (ease of fault identification and isolation), link failure only affects device(s) connected to that link, and is less expensive than mesh. Its drawbacks include more

cable requirements (than bus and ring) and single point of failure (if central device fail, the whole system will be down).

Question sources

Computer Science model exam collection · Question 18

Question 167 | SS126

Given a situation two hosts attempt on a half-duplex Ethernet LAN to send data concurrently, resulting in a collision and subsequent to this collision,
what will the hosts do?

A. An electrical pulse indicates that the collision has cleared

B. The router on the segment will signal that the collision has cleared

C. The jam signal indicates that the collision has been cleared

D. The hosts will attempt to resume transmission after a time delay has expired

Hint

Compare the signal mechanism, medium properties or transmission direction against the definitions and stated physical assumptions.

Answer D: Stop and retry after random backoff

NET14 gives the collision sequence: detect, jam, stop and retry after random backoff. The jam indicates the collision itself, not that it has cleared. There is no router-coordinated clearance procedure or electrical clearance pulse in the stated rule. Therefore waiting for a delay and attempting transmission again is the supported host behavior.

Why each choice is right or wrong

A - Incorrect: The defined procedure uses collision indication and backoff; it does not include a collision-cleared electrical pulse.

B - Incorrect: Ethernet collision recovery is performed by the hosts' MAC procedure, not a router clearance signal.

C - Incorrect: A jam announces the collision; it does not certify that the shared medium is clear.

D - Correct: After stopping, hosts retry following random backoff, matching a delay before another transmission attempt.

Primary note proof

Study-note section NET14

Random access allows contention: ALOHA sends opportunistically; CSMA senses before sending. In legacy half-duplex Ethernet, CSMA/CD detects collision, sends a jam indication, stops, and retries after random backoff. The jam signals a collision, not its clearance. Wi-Fi 802.11 uses

CSMA/CA with waiting/backoff and acknowledgments; sensing does not eliminate hidden-terminal collisions.

Study-note section NET14

Controlled access uses polling, reservations or a token to grant turns; correctly coordinated access avoids contention collisions. Channelization divides frequency, time or code resources. Stop-and-wait sends one frame and waits for ACK, retransmitting on timeout; sequence bits distinguish duplicates. Sliding windows permit multiple unacknowledged frames. Link reliability/flow control is hop-local; transport reliability/flow control is end-to-end. Ethernet detects corruption but does not itself guarantee reliable delivery.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 21 | lines 6-26

MEDIUM ACCESS CONTROL
The problem of controlling the access to the medium is similarto the rules of speaking in a meeting (the right to speak isupheld; two people do not speak at the same time; do notinterrupt each other; do not monopolize the discussion; ...) Three categories of multiple access protocols
Random Access Protocols - try your best like taxis do
• MA - Multiple Access
• CSMA - Carrier Sense MA
• CSMA/CD - CSMA with Collision Detection
• CSMA/CA - CSMA with Collision AvoidanceControlled-Access Protocols - get permission
• Reservation
• Polling
• Token Passing
Channelization Protocols - simultaneous use
• FDMA - Frequency-Division MA
• TDMA - Time-Division MA
• CDMA - Code-Division MA

Data Communication and Computer Networking module | PDF page 12 | lines 17-26

Active Hubs
An active hub is actually a multipart repeater. It is normallyused to create connections between stations in a physical startopology.
HUB: Hubs are commonly used to connect segments (devices)of a LAN. Hubs don‘t filter information; instead broadcast incoming packets to all computers connected to it. A hub contains multiple ports which support 8, 12 or

24 RJ-45 ports. Two types: Passive hub and Active hub. It is used in star or ring topology.

Question sources

Computer Science model exam collection · Question 33

Question 168 | SS134

Which of the following is true regarding the use of switches and hubs for network connectivity in the network?

A. Switches increase the number of collision domains in the network

B. Switches take less time to process frames than hubs take

C. Switches do not forward broadcasts

D. Hubs can filter frames

Hint

Compare signal repetition, frame forwarding, packet routing and policy enforcement using the stated device or traffic assumptions.

Answer A: Switch ports separate collision domains

NET10 says each switch port separates collision domains, whereas a half-duplex hub repeats traffic into one shared collision domain. Switches still flood broadcasts within their VLAN, and hubs do not inspect and filter destination frames. The note gives no universal switch-versus-hub processing-time advantage, so A is the supported claim.

Why each choice is right or wrong

A - Correct: Replacing a shared hub segment with separate switch ports divides the network into additional collision domains.

B - Incorrect: The note establishes no universal lower switch processing time; a hub simply repeats signals.

C - Incorrect: Switches flood broadcasts within the VLAN unless another control filters them.

D - Incorrect: Hubs repeat physical signals and neither learn MAC destinations nor filter frames.

Primary note proof

Study-note section NET10

Each switch port separates collision domains; full-duplex point-to-point Ethernet has no collisions and does not use CSMA/CD. Switching permits independent conversations simultaneously. Broadcasts still reach the VLAN unless another control filters them. A layer-3 switch also routes, so device marketing names do not override the function being examined.

Study-note section NET09

A repeater regenerates layer-1 signals without inspecting destination addresses. An active hub is a multiport repeater: it repeats incoming signals onto other ports, placing half-duplex endpoints in one collision domain. A passive hub is a connector. A hub neither learns MAC addresses nor eliminates collisions. An endpoint such as a network printer consumes services; routers, hubs and access points are intermediary devices.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 12 | lines 17-26

Active Hubs
An active hub is actually a multipart repeater. It is normallyused to create connections between stations in a physical startopology.
HUB: Hubs are commonly used to connect segments (devices)of a LAN. Hubs don‘t filter information; instead broadcast incoming packets to all computers connected to it. A hub contains multiple ports which support 8, 12 or 24 RJ-45 ports. Two types: Passive hub and Active hub. It is used in star or ring topology.

Data Communication and Computer Networking module | PDF page 12 | lines 27-37

SWITCH: A switch filters and forwards data packets across anetwork.
Unlike a hub which simply replicates what it receives on oneport onto all the other ports, a switch keeps a record of the MAC addresses of the devices attached to it.
When the switch receives a data packet, it forwards the packetdirectly to the recipient device by looking up the MAC address.
• Switch is intelligent and expensive than Hub
• Switch is a point to point communication device
• Hub is a broadcasting device

Data Communication and Computer Networking module | PDF page 13 | lines 2-8

Filters content by reading the MAC addresses of source and destination.
• MAC to Segment number table
• Do not filter broadcast
• Data not destined for other network is prevented from passing over the bridge
• Slower than repeater due to filtering

Question sources

Computer Science model exam collection · Question 41

Question 169 | SS145

A TCP/IP layer which is responsible for addressing, path selection and routing refers:

A. Transport Layer

B. Network Access Layer

C. Application Layer

D. Internet Layer

Hint

Match the requested scope or data unit to the layer duties in the note; distinguish hop delivery from end-to-end process delivery.

Answer D: Internet Layer

The TCP/IP Internet layer corresponds to OSI network and provides IP addressing/source-to-destination transmission with routing. Evidence: PDF 17, 15, 17.

Why each choice is right or wrong

A - Incorrect: Transport is process delivery (PDF 17, 15, 17.)

B - Incorrect: Network access combines physical/data link (PDF 17, 15, 17.)

C - Incorrect: Application combines OSI upper layers (PDF 17, 15, 17.)

D - Correct: Internet matches network-layer addressing and routing (PDF 17, 15, 17.)

Primary note proof

Study-note section NET19

> The four-layer TCP/IP model folds OSI layers 5-7 into application, retains transport, calls layer 3 Internet, and combines link/physical as network access. A model is a guide to functions, not a guarantee that every application gets a reliable network. Distinguish end-to-end application service from its underlying process-to-process transport.

Study-note section NET30

> Routing computes paths; forwarding chooses a next hop for an individual packet. Select the matching route with the longest prefix, then apply the routing system's tie-breaking criteria. A default /0 matches when nothing more specific does. Static routes are configured; dynamic protocols exchange reachability. Distance vector uses neighbor estimates, while link state distributes link information and computes shortest paths. Interior protocols operate within an autonomous system; BGP exchanges routes between systems.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 17 | lines 22-38

> Network Layer or IP
> Also called as the Internetwork Layer (IP). It holds the

IP protocol which is a network layer protocol and is responsiblefor source to destination transmission of data.
The Internetworking Protocol (IP) is a connection-less & unreliable protocol.
It is a best effort delivery service. i.e. there is no error checking in IP, it simply sends the data and relies on its underlying layers to get the data transmitted to the destination.Even if it is unreliable IP cannot be considered weak and useless; since it provides only the functionality that is requiredfor transmitting data thereby giving maximum efficiency.
Since there is no mechanism of error detection or correction in IP, there will be no delay introduced on a medium where thereis no error at all.

Data Communication and Computer Networking module | PDF page 15 | lines 41-61

Network Layer
• The network layer makes sure that the data is deliveredto the receiver despite multiple intermediate devices.
• The network layer at the sending side accepts data from the transport layer, divides it into packets, addsaddressing information in the header and passes it tothe data link layer.
• The network layer is responsible for source todestination of delivery of data.
• The network layer uses logical address commonlyknown as IP address to recognize devices on the network.
• Each packet is independent of the other and may travelusing different routes to reach the receiver hence may arrive out of turn at the receiver (Routing).
• The Network layer does not perform any flow controlor error control
• The main responsibility of Network Layer is transmission of packets from source to destination

Data Communication and Computer Networking module | PDF page 17 | lines 3-15

The structure TCP/IP model is very similar to the structure of the OSI reference model. The OSI model has seven layers where the TCP/IP model has four layers.
• The Application layer of TCP/IP model corresponds to the Application Layer of Session, Presentation & Application Layer of OSI model.

• The Transport layer of TCP/IP model corresponds to theTransport Layer of OSI model
• The Network layer of TCP/IP model corresponds to the Network Layer of OSI model
• The Host to network layer of TCP/IP model correspondsto the Physical and Data link Layer of OSI model.

Question sources

Computer Science model exam collection · Question 52

Question 170 | SS170

Which of the following is the correct order of packet data unit as data moved in the OS! reference model from bottom to top?

A. Segment, packet, frame, bit

B. Segment, frame, packet, bit

C. Bit, packet, frame, segment

D. Bit, frame, packet, segment

Hint

Match the requested scope or data unit to the layer duties in the note; distinguish hop delivery from end-to-end process delivery.

Answer D: Bit, frame, packet, segment

Moving bottom to top reverses sending encapsulation: physical bits become data-link frames, then network packets, then transport segments. Evidence: PDF 14, 15, 15, 16.

Why each choice is right or wrong

A - Incorrect: Starts at transport instead of physical and moves downward

B - Incorrect: Starts at transport and misorders frame and packet

C - Incorrect: Skips frame before packet

D - Correct: Bit, frame, packet, segment follows the upward layer order

Primary note proof

Study-note section NET12

Sending proceeds from application data to transport segment/datagram, network packet, link frame and physical bits/symbols; receiving reverses the order. Each layer serves the layer above. A router removes a received link frame, inspects IP, and creates a new link frame for the next hop. MAC addresses usually change across routed hops; end-to-end IP addresses ordinarily remain until translation.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 14 | lines 32-49

Physical Layer:
• The Physical Layer provides a standardized interface to physical transmission media, including: Mechanical specification of electrical connectors and cables, for example maximum cable length, Electrical specification of transmission line and Bit-by-bit or symbol-by-symbol delivery.
• Interface: The Physical Layer defines the characteristics of interfaces between the devices & transmission medium.
• Representation of bits: The physical layer is concerned with transmission of signals from one device to another which involves converting data (1_s & 0_s) into signals and vice versa. It is not concerned with the meaning or interpretation of bits.
• Data rate: The physical layer defines the data transmission rate i.e. number of bits sent per second. It is the responsibility of the physical layer to maintain the defined data rate.

Data Communication and Computer Networking module | PDF page 15 | lines 13-40

Data Link Layer
• The Data Link layer adds reliability to the physical layer by providing error detection and correction mechanisms.
• Framing: the Data Link layer receives the data from Network Layer and divides the stream of bits into fixed size manageable units called as Frames and sends it to the physical layer. On the receiver side, the data link layer receives the stream of bits from the physical layer and regroups them into frames and sends them to the Network layer.
• Physical Addressing: The Data link layer appends the physical address in the header of the frame before sending it to physical layer.
• Flow control: The data link layer makes sure that the sender sends the data at a speed at which the receiver canreceive it else if there is an overflow at the receiver sidethe data will be lost.
• Error Control: The data link layer imposes error control mechanism to identify lost or damaged frames, duplicateframes and then retransmit them.
• Access Control: The data link layer imposes access control mechanism to determine which

device has right to send data in an multipoint connection setting.
• Main Responsibility: The main responsibility of the data link layer is hop to hop transmission of frames.

Data Communication and Computer Networking module | PDF page 15 | lines 41-61

Network Layer
• The network layer makes sure that the data is deliveredto the receiver despite multiple intermediate devices.
• The network layer at the sending side accepts data from the transport layer, divides it into packets, addsaddressing information in the header and passes it tothe data link layer.
• The network layer is responsible for source todestination of delivery of data.
• The network layer uses logical address commonlyknown as IP address to recognize devices on the network.
• Each packet is independent of the other and may travelusing different routes to reach the receiver hence may arrive out of turn at the receiver (Routing).
• The Network layer does not perform any flow controlor error control
• The main responsibility of Network Layer is transmission of packets from source to destination

Data Communication and Computer Networking module | PDF page 16 | lines 2-17

• At the sending side, the transport layer receives data from the session layer, divides it into units called segments and sends it to the network layer.
• To ensure process to process delivery the transport layer makes use of port address to identify the data from the sending and receiving process.
• The data can be transported in a connection oriented or connectionless manner.
• The Transport layer is responsible for segmentation and reassembly of the message into segments which bear sequence numbers.
• The transport layer also carries out flow control and error control functions; but unlike data link layer these are end to end rather than node to node.
• The main responsibility of the transport layer is process to process delivery of the entire message

Question sources

Computer Science model exam collection · Question 77

Question 171 | AM0474

Which of the following is not a primary function of the network layer in the OSI model?

A. Routing

B. Addressing

C. Flow control

D. Fragmentation

Hint

Match the requested scope or data unit to the layer duties in the note; distinguish hop delivery from end-to-end process delivery.

Answer C: Flow control is not a primary network-layer duty

The network layer supplies logical addressing/routing and, for IPv4, fragmentation when permitted. Flow control instead protects a receiver in transport or hop-local link procedures, as NET14 and NET17 explain. Thus C is not a primary network-layer function in this layer model, without claiming that all control mechanisms belong exclusively to one layer.

Why each choice is right or wrong

A - Incorrect: Routing is explicitly a main network-layer duty in the NET12 layer table.

B - Incorrect: Logical addressing is explicitly assigned to the network layer.

C - Correct: Receiver flow control is described at link and transport scope rather than as a primary network duty.

D - Incorrect: NET16 supports IPv4 fragmentation by sources and routers, a network-protocol function.

Primary note proof

Study-note section NET16

> The IPv4 checksum protects its header; IP does not lack error checking altogether. Identification, flags and offset support fragmentation. IPv4 sources and routers may fragment when allowed; reassembly occurs at the destination. If DF is set and the next MTU is too small, forwarding fails and an ICMP diagnostic may be returned.

Study-note section NET14

> Controlled access uses polling, reservations or a token to grant turns; correctly coordinated access avoids contention collisions. Channelization divides frequency, time or code resources. Stop-and-wait sends one frame and waits for ACK, retransmitting on timeout; sequence bits distinguish duplicates. Sliding windows permit multiple unacknowledged frames. Link

reliability/flow control is hop-local; transport reliability/flow control is end-to-end. Ethernet detects corruption but does not itself guarantee reliable delivery.

Study-note section NET17

TCP offers a reliable ordered byte stream using sequence numbers, acknowledgments, retransmission and windows. Flow control protects the receiver; congestion control protects network capacity. UDP sends independent datagrams with ports and a checksum but no built-in setup, delivery guarantee, retransmission or ordering. Live interactive traffic may choose UDP when late data is less useful than lost data. Application protocols can add reliability over UDP.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 15 | lines 41-61

Network Layer
• The network layer makes sure that the data is deliveredto the receiver despite multiple intermediate devices.
• The network layer at the sending side accepts data from the transport layer, divides it into packets, addsaddressing information in the header and passes it tothe data link layer.
• The network layer is responsible for source todestination of delivery of data.
• The network layer uses logical address commonlyknown as IP address to recognize devices on the network.
• Each packet is independent of the other and may travelusing different routes to reach the receiver hence may arrive out of turn at the receiver (Routing).
• The Network layer does not perform any flow controlor error control
• The main responsibility of Network Layer is transmission of packets from source to destination

Data Communication and Computer Networking module | PDF page 16 | lines 2-17

• At the sending side, the transport layer receives data from the session layer, divides it into units called segments and sends it to the network layer.
• To ensure process to process delivery the transport layer makes use of port address to identify the data from the sending and receiving process.
• The data can be transported in a connection oriented or connectionless manner.
• The Transport layer is responsible for segmentation and reassembly of the message into segments which

bear sequence numbers.
• The transport layer also carries out flow control and error control functions; but unlike data link layer these are end to end rather than node to node.
• The main responsibility of the transport layer is process to process delivery of the entire message

Question sources

Computer Science MCQ practice collection · Question 474

Question 172 | AM0475

What is the purpose of a MAC address in computer networking?

A. To identify a device within a local area network (LAN)

B. To identify a device within a wide area network (WAN)

C. To establish a secure connection between two devices

D. To determine the IP address of a device

Hint

Use the cited note definitions to identify the requested function or scope, then check each alternative against that same rule.

Answer A: To identify a device within a local area network (LAN)

The module physical MAC address is imprinted on a NIC and used for local physical delivery; it is not encryption or the IP routing address. Evidence: PDF 17, 15.

Why each choice is right or wrong

A - Correct: MAC identifies the local physical interface for frame delivery (PDF 17, 15.)

B - Incorrect: WAN-wide logical routing uses IP rather than treating MAC as a universal end-to-end address (PDF 17, 15.)

C - Incorrect: A physical identifier does not establish encryption/security (PDF 17, 15.)

D - Incorrect: ARP starts with IP and resolves MAC; MAC itself is not a rule for determining IP (PDF 17, 15.)

Primary note proof

Study-note section NET20

ARP resolves an on-link IPv4 next hop to a link address, using a broadcast request and normally unicast reply. For an off-subnet target, ARP resolves the gateway, not the remote target's MAC. It bridges the network/link addressing boundary and is often classified at the link layer; calling ARP simply a network protocol uses a loose textbook convention. RARP reverses hardware-to-IP lookup; BOOTP/DHCP support boot configuration. ICMP reports errors and diagnostics; IGMP

manages IPv4 multicast membership. These are separate companion protocols, not four pieces whose combination is IP.

Study-note section NET10

A bridge or ordinary Ethernet switch operates at layer 2. It learns source-MAC-to-port mappings, looks up the destination, forwards a known unicast to its port, filters it if the destination is on the incoming segment, and floods an unknown unicast or broadcast within its VLAN. A switch does not always send only to one destination port. Wireless access points normally bridge wireless and wired link-layer traffic.

Study-note section NET12

Sending proceeds from application data to transport segment/datagram, network packet, link frame and physical bits/symbols; receiving reverses the order. Each layer serves the layer above. A router removes a received link frame, inspects IP, and creates a new link frame for the next hop. MAC addresses usually change across routed hops; end-to-end IP addresses ordinarily remain until translation.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 17 | lines 44-53

ARP - Address Resolution Protocol: It is used to
resolve thephysical address of a device on a network,
where its logical address is known.
Physical address is the 48 bit address that is imprinted
on theNIC or LAN card, Logical address is the Internet
Address orcommonly known as IP address that is used
to uniquely & universally identify a device.
RARP- Reverse Address Resolution Protocol: It is
used bya device on the network to find its Internet
address when it knows its physical address.

Data Communication and Computer Networking module | PDF page 15 | lines 13-40

Data Link Layer
• The Data Link layer adds reliability to the physical
layer by providing error detection and correction
mechanisms.
• Framing: the Data Link layer receives the data
from Network Layer and divides the stream of bits
into fixed size manageable units called as Frames
and sends it to the physical layer. On the receiver
side, the data link layer receives the stream of bits
from the physical layer and regroups them into
frames and sends them to the Network layer.
• Physical Addressing: The Data link layer appends
the physical address in the header of the frame
before sending it to physical layer.

• Flow control: The data link layer makes sure that the sender sends the data at a speed at which the receiver canreceive it else if there is an overflow at the receiver sidethe data will be lost.
• Error Control: The data link layer imposes error control mechanism to identify lost or damaged frames, duplicateframes and then retransmit them.
• Access Control: The data link layer imposes access control mechanism to determine which device has right to send data in an multipoint connection setting.
• Main Responsibility: The main responsibility of the data link layer is hop to hop transmission of frames.

Question sources

Computer Science MCQ practice collection · Question 475

Question 173 | AM0476

Which of the following protocols is used for email transmission?

A. FTP (File Transfer Protocol)

B. SMTP (Simple Mail Transfer Protocol)

C. HTTP (Hypertext Transfer Protocol)

D. DNS (Domain Name System)

Hint

Identify the requested service or delivery guarantee, then distinguish application roles, transport behavior and address configuration.

Answer B: SMTP (Simple Mail Transfer Protocol)

SMTP is explicitly Simple Mail Transfer Protocol in the application list, matching email transmission. Evidence: PDF 18, 28.

Why each choice is right or wrong

A - Incorrect: FTP transfers files (PDF 18, 28.)

B - Correct: SMTP is the explicitly named mail transfer protocol (PDF 18, 28.)

C - Incorrect: HTTP is the web service in the port table (PDF 18, 28.)

D - Incorrect: DNS is external naming (PDF 18, 28.)

Primary note proof

Study-note section NET21

HTTP defines web request/response semantics; it is stateless, and a message body may be absent. HTTPS adds TLS protection. FTP transfers files using control and separate data connections; it is not the same protocol as SFTP. SMTP submits and relays mail; POP3 retrieves messages and IMAP accesses/synchronizes server mailboxes. Saying SMTP handles both sending and end-user mailbox retrieval is inaccurate.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 18 | lines 27-32

Application Layer
The Application Layer is a combination of Session,
Presentation & Application Layers of OSI models and defines
high level protocols like File Transfer (FTP), Electronic Mail
(SMTP), Virtual Terminal (TELNET), Domain Name Service
(DNS), etc.

Data Communication and Computer Networking module | PDF page 28 | lines 32-45

Application Layer
The application layer in TCP/IP is equivalent to the
combined session, presentation, and application layers in
the OSI model and many protocols are defined at this
layer.
The Process/Application Layer Protocols
• Telnet
• File Transfer Protocol (FTP)
• Network File System (NFS).
• Simple Mail Transfer Protocol (SMTP
• POP3 is used to receive mail.
• Simple Network Management Protocol (SNMP)
• Domain Name Service (DNS)
• Dynamic Host Configuration Protocol (DHCP)

Question sources

Computer Science MCQ practice collection · Question 476

Question 174 | AM0477

What is the purpose of a firewall in computer networks?

A. To encrypt network traffic for secure communication

B. To manage network resources and allocate bandwidth

C. To filter and control network traffic based on predefined rules

D. To connect two separate networks and enable communication between them

Hint

Use the cited note definitions to identify the requested function or scope, then check each alternative against that same rule.

Answer C: To filter and control network traffic based on predefined rules

The module firewall example permits only authorized systems to access internal computers, supporting selective traffic filtering/control. Evidence: PDF 48, 12, 16.

Why each choice is right or wrong

A - Incorrect: Encryption is a distinct presentation function (PDF 48, 12, 16.)

B - Incorrect: Bandwidth allocation is not the firewall access-control function described (PDF 48, 12, 16.)

C - Correct: Rules permitting authorized access match firewall filtering (PDF 48, 12, 16.)

D - Incorrect: Connecting networks is the router/gateway function, not the defining firewall policy (PDF 48, 12, 16.)

Primary note proof

Study-note section NET11

> A firewall allows, rejects or inspects traffic under a security policy; it does not necessarily encrypt. A VPN, Virtual Private Network, provides a logical private connection over another network; a secure VPN authenticates/encrypts its tunnel. A modem modulates outgoing and demodulates incoming carrier signals. These functions may coexist in one home router but remain conceptually distinct.

Study-note section NET11

> Routers forward IP packets between networks using destination prefixes and next hops. They separate broadcast domains and normally do not forward local link broadcasts. A default gateway is usually a router, while a protocol gateway can translate application formats; therefore a gateway is not inherently a device that implements every OSI layer.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 48 | lines 29-40

> Network Address Translation (NAT)
> NAT translates the IP addresses of computers in a local network to a single IP address. This address is often used by the router that connects the computers to the Internet. The router can be connected to a DSL modem, cable modem, T1 line, or even a dial-up modem. When other computers on the Internet attempt to access computers within the local network, they only see the IP address of the router. This adds an extra level of security, since the router can be configured as a firewall, only allowing

authorized systems to access the computers within the network.

Data Communication and Computer Networking module | PDF page 12 | lines 38-52

ROUTER: Router is a specialized network device used tointerconnect different types of network that uses different protocol.
Router allows the users to connect several LAN and WAN
• A LAN to another LAN
• A WAN to another WAN
• A LAN to the Internet
Routers use the routing table to determine how to forwardpackets.
• The list of routing tables provides directions to transfer the data to a particular network destination -various paths to forward the data.
• A router analyzes a destination IP address of a givenpacket and compares it with the routing table to decide the packet's next best path

Data Communication and Computer Networking module | PDF page 16 | lines 33-42

Presentation Layer
• The communicating devices may be having different platforms. The presentation layer performs translation, encryption and compression of data.
• The presentation layer receives the data from the application layer adds header which contains information related to encryption and compression and sends it to the session layer.
• So, the main responsibility of the Presentation layer is translation, compression and encryption.

Question sources

Computer Science MCQ practice collection · Question 477

Question 175 | AM0478

Which of the following network topologies provides the highest fault tolerance?

A. Bus topology

B. Ring topology

C. Star topology

D. Mesh topology

Hint

Draw the links and identify shared components, alternate paths and the effect of the specified failure or growth requirement.

Answer D: Mesh topology

Mesh has redundant interconnections and a single link failure does not affect the entire network. Bus backbone, ring break and star center failure are explicit vulnerabilities. Evidence: PDF 23, 24, 23, 23, 23.

Why each choice is right or wrong

A - Incorrect: A broken backbone can shut down bus (PDF 23, 24, 23, 23, 23.)

B - Incorrect: A break/disabled station can disable a ring (PDF 23, 24, 23, 23, 23.)

C - Incorrect: Central device failure can shut down star (PDF 23, 24, 23, 23, 23.)

D - Correct: Redundant mesh paths support the strongest listed fault tolerance (PDF 23, 24, 23, 23, 23.)

Primary note proof

Study-note section NET08

> Bus uses a shared backbone; an unterminated break can disrupt the segment. Star connects endpoints through a central device: one edge failure isolates that endpoint, whereas central failure affects the star. Ring forms a loop; basic single rings are vulnerable to a break, while protected dual rings differ. Token passing is associated with Token Ring but is an access method, not a necessary property of every ring. Tree is hierarchical; hybrid combines arrangements.

Study-note section NET08

> A full undirected mesh of n nodes needs n(n-1)/2 links and n-1 interfaces per node. For 50 nodes: 50×49/2=1225 links. Redundant paths improve fault tolerance at greater cable and interface cost.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 23 | lines 45-53

> Mesh Topology: in this topology devices are
> connected with many redundant interconnections
> between network nodes. In a full mesh topology,
> every node has a connection to every other node in
> the network, which makes it the most expensive
> topology over all the other topologies. The number of
> cables grows fast as the number of nodes increases,
> and it can be calculated by using the general formula
> ((n (n - 1)) /2), where n is the number of nodes in the

Data Communication and Computer Networking module | PDF page 24 | lines 2-10

network. It has several benefits, such as: dedicated links between devices, robust (single link failure don‘t affect entire network), privacy/security (direct communication between communicating devices), and ease of fault identification and isolation. Its drawbacks include, installation and reconnection are difficult (large number of cables), huge amount of cables consumes a lot of space, and it is the most expensive of all.

Data Communication and Computer Networking module | PDF page 23 | lines 19-34

Star Topology: in this topology, each node is connected directly to a central device called a hub or a switch. Data on a star network passes through the central device (switch) before continuing to its destination. The central device manages and controls all functions of the network. This configuration is common with twisted pair cable. RJ-45 Connectors are used to connect the cable to the Network Interface Card (NIC) of each computer. Its advantages include, ease of installation and reconfiguration, robust (ease of fault identification and isolation), link failure only affects device(s) connected to that link, and is less expensive than mesh. Its drawbacks include more cable requirements (than bus and ring) and single point of failure (if central device fail, the whole system will be down).

Data Communication and Computer Networking module | PDF page 23 | lines 35-44

Ring Topology: in this topology, all devices are connected to one another in the shape of a closed loop, so that each device is connected directly to two other devices, one on either side of it. Some of its advantages include, easy to install and reconfigure, less expensive (than mesh), and performance is even despite the number of users. Its cons include, break in the ring (such as a disabled station) can disable the entire network, and limitations on media and traffic (limitation on ring length and number of devices).

Data Communication and Computer Networking module | PDF page 23 | lines 4-18

Bus Topology: in this topology all devices are connected to a central cable, called the bus or backbone, which is terminated at its ends. The purpose of the terminators is to stop the signal from bouncing, thereby clearing the cable so that other computers can send data. Message transmitted along

the Bus is visible to all computers connected to the backbone cable. As the message arrives at each workstation, the workstation checks the destination address contained in the message either to process or drop the packet if it matches or not respectively. Its advantages are, ease of installation and less amount of cable requirement. Its main drawback is, the entire network will be shut down if there is a break in the main cable.

Question sources

Computer Science MCQ practice collection · Question 478

Question 176 | AM0479

Which listed terms describe IPv6's flexible-prefix addressing or operations supported by that approach? Select all that apply.

A. Classful addressing

B. Classless addressing

C. Subnetting

D. CIDR (Classless Inter-Domain Routing)

Hint

Identify the requested service or delivery guarantee, then distinguish application roles, transport behavior and address configuration.

Answer B, C, D: Classless addressing; Subnetting; CIDR (Classless Inter-Domain Routing)

IPv6 uses flexible network prefixes rather than historical IPv4 address classes. Classless addressing describes this approach, subnetting divides prefixes into smaller networks, and CIDR terminology expresses classless prefixes and aggregation. These are compatible descriptions or operations rather than mutually exclusive schemes. The selection instruction therefore permits all three while excluding the classful A/B/C allocation model associated with historical IPv4.

Why each choice is right or wrong

A - Incorrect: Historical classful A/B/C IPv4 defaults are not the IPv6 flexible-prefix scheme.

B - Correct: IPv6 uses flexible prefixes rather than fixed historical address classes.

C - Correct: IPv6 prefixes can be subdivided into subnets; the term overlaps the broad scheme wording.

D - Correct: Classless prefix/CIDR terminology applies to flexible-prefix allocation and routing rather than historical class boundaries.

Primary note proof

Study-note section NET23

IPv6 has 128-bit hexadecimal addresses, flexible prefixes and no IPv4-style broadcast. Sources, not routers, fragment IPv6 packets. IPv6 does not automatically encrypt traffic or make authentication unnecessary. Compare IPv6's larger 128-bit address space and encryption support separately; specify the property being evaluated.

Study-note section NET28

CIDR, Classless Inter-Domain Routing, replaces rigid class allocation and supports aggregation. Combine contiguous aligned blocks sharing leading bits; unrelated adjacent-looking labels may not aggregate cleanly. Four consecutive /26 blocks covering a /24 summarize to /24. More-specific routes must remain available where the aggregate would otherwise send traffic to the wrong next hop.

Study-note section NET26

To split parent /a into equal /p blocks, borrow b=p-a bits and obtain 2^b subnets. Do not subtract two subnets under modern practice. For a Class B /16 parent split to /19, b=3 gives eight subnets, each with 8192 addresses and 8190 conventional hosts. A /19 alone does not state its parent.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 19 | lines 37-44

CIDR: A class B address is far too large for most
organizationsand a class C network, with 256 addresses is
too small. This leads to granting Class B address to
organizations who do not require all. This is resulting in
depletion of Address space. A solution is CIDR (Classless
InterDomain Routing) The basic idea behind CIDR, is to
allocate the remaining IP addresses in variable-sized
blocks, without regard to the classes.

Data Communication and Computer Networking module | PDF page 19 | lines 45-49

NAT (Network Address Translation): The scarcity of
network addresses in IPv4 led to the development of IPv6.
Due to this, we need to use private IP address inside the
organization and translate it to public IP address using
NAT.

Question sources

Computer Science MCQ practice collection · Question 479

Question 177 | AM0480

Which protocol is responsible for translating domain names into IP addresses?

A. DHCP (Dynamic Host Configuration Protocol)

B. DNS (Domain Name System)

C. ARP (Address Resolution Protocol)

D. ICMP (Internet Control Message Protocol)

Hint

Identify the requested service or delivery guarantee, then distinguish application roles, transport behavior and address configuration.

Answer B: DNS (Domain Name System)

DNS is the domain naming service and external name/address service contrasted with hosts entries. Evidence: PDF 18, 65, 28, 17, 17.

Why each choice is right or wrong

A - Incorrect: DHCP is named host configuration, not domain naming

B - Correct: DNS matches the named domain service

C - Incorrect: ARP resolves known IP to MAC

D - Incorrect: ICMP reports packet problems

Primary note proof

Study-note section NET20

> DNS resolves names to records, including IPv4 A and IPv6 AAAA addresses; it can use UDP or TCP port 53. DHCP dynamically leases IPv4 settings, commonly address, mask, gateway and DNS server. Its basic exchange is discover, offer, request, acknowledge. IP itself does not assign addresses.

Study-note section NET20

> ARP resolves an on-link IPv4 next hop to a link address, using a broadcast request and normally unicast reply. For an off-subnet target, ARP resolves the gateway, not the remote target's MAC. It bridges the network/link addressing boundary and is often classified at the link layer; calling ARP simply a network protocol uses a loose textbook convention. RARP reverses hardware-to-IP lookup; BOOTP/DHCP support boot configuration. ICMP reports errors and diagnostics; IGMP manages IPv4 multicast membership. These are separate companion protocols, not four pieces whose combination is IP.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 18 | lines 27-32

Application Layer
The Application Layer is a combination of Session, Presentation & Application Layers of OSI models and defines high level protocols like File Transfer (FTP), Electronic Mail (SMTP), Virtual Terminal (TELNET), Domain Name Service (DNS), etc.

Data Communication and Computer Networking module | PDF page 65 | lines 31-38

/etc/hosts
The /etc/hosts file always contains the localhost IP address, 127.0.0.1, which is
usedfor interprocess communication.
Never remove this line! Sometimes contains addresses of additional hosts, whichcan be contacted without using an external naming service such as DNS (the Domain Name Server).

Data Communication and Computer Networking module | PDF page 28 | lines 32-45

Application Layer
The application layer in TCP/IP is equivalent to the combined session, presentation, and application layers in the OSI model and many protocols are defined at this layer.
The Process/Application Layer Protocols
• Telnet
• File Transfer Protocol (FTP)
• Network File System (NFS).
• Simple Mail Transfer Protocol (SMTP
• POP3 is used to receive mail.
• Simple Network Management Protocol (SNMP)
• Domain Name Service (DNS)
• Dynamic Host Configuration Protocol (DHCP)

Data Communication and Computer Networking module | PDF page 17 | lines 44-53

ARP - Address Resolution Protocol: It is used to resolve thephysical address of a device on a network, where its logical address is known.
Physical address is the 48 bit address that is imprinted on theNIC or LAN card, Logical address is the Internet Address orcommonly known as IP address that is used to uniquely & universally identify a device.
RARP- Reverse Address Resolution Protocol: It is used bya device on the network to find its Internet address when it knows its physical address.

Data Communication and Computer Networking module | PDF page 17 | lines 54-59

ICMP- Internet Control Message Protocol: It is a signaling mechanism used to inform the sender about datagram problemsthat occur during transit. It is used by intermediate devices.
IGMP- Internet Group Message Protocol: It is a mechanism that allows sending the same message to a group of recipients.

Question sources

Computer Science MCQ practice collection · Question 480

Question 178 | AM0481

What is the purpose of NAT (Network Address Translation) in computer networks?

A. To secure network communications through encryption

B. To provide redundancy and fault tolerance

C. To translate private IP addresses to public IP addresses

D. To manage network resources and allocate bandwidth

Hint

Convert the mask to a prefix, separate network and host bits, and apply the relevant subnet-count or usable-host rule.

Answer C: To translate private IP addresses to public IP addresses

NAT explicitly translates an organization private IP address to a public IP address. It is not an encryption, redundancy or bandwidth-allocation mechanism. Evidence: PDF 19, 48, 16.

Why each choice is right or wrong

A - Incorrect: Encryption is a separate representation/security transformation (PDF 19, 48, 16.)

B - Incorrect: Redundancy is not the address translation definition (PDF 19, 48, 16.)

C - Correct: Private-to-public translation is the exact NAT definition (PDF 19, 48, 16.)

D - Incorrect: Bandwidth allocation is not the NAT definition (PDF 19, 48, 16.)

Primary note proof

Study-note section NET29

Static NAT gives a fixed address mapping; dynamic NAT allocates mappings from a pool. PAT/NAPT maps address-plus-port combinations so multiple private clients share a public address. It is translation, not ARP resolution and not encryption. Return traffic must match the translation state or a configured inbound mapping.

Study-note section NET29

A private host such as 10.0.0.1 commonly reaches the public Internet through NAT at a gateway, together with valid routing and a public external address. NAT alone does not supply a physical

connection or DNS. A public address does not automatically grant permission to use it; both public and private unicast addresses can be used on a LAN under the correct allocation and subnet.

Study-note section NET11

A firewall allows, rejects or inspects traffic under a security policy; it does not necessarily encrypt. A VPN, Virtual Private Network, provides a logical private connection over another network; a secure VPN authenticates/encrypts its tunnel. A modem modulates outgoing and demodulates incoming carrier signals. These functions may coexist in one home router but remain conceptually distinct.

Related reading (context, not primary note proof)

Study-note section NET20

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 19 | lines 45-49

NAT (Network Address Translation): The scarcity of network addresses in IPv4 led to the development of IPv6. Due to this, we need to use private IP address inside the organization and translate it to public IP address using NAT.

Data Communication and Computer Networking module | PDF page 48 | lines 29-40

Network Address Translation (NAT)
NAT translates the IP addresses of computers in a local network to a single IP address. This address is often used by the router that connects the computers to the Internet. The router can be connected to a DSL modem, cable modem, T1 line, or even a dial-up modem. When other computers on the Internet attempt to access computers within the local network, they only see the IP address of the router. This adds an extra level of security, since the router can be configured as a firewall, only allowing authorized systems to access the computers within the network.

Data Communication and Computer Networking module | PDF page 16 | lines 33-42

Presentation Layer
• The communicating devices may be having different platforms. The presentation layer performs translation, encryption and compression of data.
• The presentation layer receives the data from the application layer adds header which contains information related to encryption and compression and sends it to the session layer.

• So, the main responsibility of the Presentation layer is translation, compression and encryption.

Variant 1 | Alternative version 1

What is the purpose of NAT (Network Address Translation) in computer networks?

A. To encrypt network traffic for secure communication

B. To assign unique IP addresses to hosts in a network

C. To provide a firewall for network security

D. To translate private IP addresses to public IP addresses

Answer D: To translate private IP addresses to public IP addresses

Apply the same study-note rule to this alternative source set; the choice contrasts below show the derivation.

Why each choice is right or wrong

A - Incorrect: Encryption changes data protection; NAT changes addresses (PDF19,48).

B - Incorrect: Assigning initial unique host addresses is different from translating already-used internal addresses (PDF19,48).

C - Incorrect: PDF48 says a router can additionally be a firewall; optional access control is not the NAT translation definition.

D - Correct: This variant moves the explicit private-to-public translation definition to D (PDF19).

Primary note proof

Study-note section NET29

Static NAT gives a fixed address mapping; dynamic NAT allocates mappings from a pool. PAT/NAPT maps address-plus-port combinations so multiple private clients share a public address. It is translation, not ARP resolution and not encryption. Return traffic must match the translation state or a configured inbound mapping.

Study-note section NET20

DNS resolves names to records, including IPv4 A and IPv6 AAAA addresses; it can use UDP or TCP port 53. DHCP dynamically leases IPv4 settings, commonly address, mask, gateway and DNS server. Its basic exchange is discover, offer, request, acknowledge. IP itself does not assign addresses.

Study-note section NET11

A firewall allows, rejects or inspects traffic under a security policy; it does not necessarily encrypt. A VPN, Virtual Private Network, provides a logical private connection over another network; a secure VPN authenticates/encrypts its tunnel. A modem modulates outgoing and demodulates incoming carrier signals. These functions may coexist in one home router but remain conceptually distinct.

Question sources

Computer Science MCQ practice collection · Question 481

Computer Science MCQ practice collection · Question 522

Question 179 | AM0482

Which listed protocol is a connectionless transport-layer protocol, sending independent datagrams without built-in connection setup?

A. TCP (Transmission Control Protocol)

B. UDP (User Datagram Protocol)

C. HTTP (Hypertext Transfer Protocol)

D. FTP (File Transfer Protocol)

Hint

Identify the requested service or delivery guarantee, then distinguish application roles, transport behavior and address configuration.

Answer B: UDP (User Datagram Protocol)

UDP is a transport protocol that sends independent datagrams without a built-in setup handshake, ordering or retransmission service. TCP instead establishes a connection and supplies an ordered reliable byte stream. HTTP and FTP are application protocols, so they are outside the requested transport-layer category. HTTP being stateless at the application level does not make it a connectionless transport protocol.

Why each choice is right or wrong

A - Incorrect: TCP is connection-oriented transport with reliable ordered byte-stream delivery.

B - Correct: UDP is the connectionless datagram transport described.

C - Incorrect: HTTP is an application protocol; application statelessness is distinct from connectionless transport.

D - Incorrect: FTP is an application file-transfer protocol, not a transport protocol.

Primary note proof

Study-note section NET17

> TCP offers a reliable ordered byte stream using sequence numbers, acknowledgments, retransmission and windows. Flow control protects the receiver; congestion control protects network capacity. UDP sends independent datagrams with ports and a checksum but no built-in setup, delivery guarantee, retransmission or ordering. Live interactive traffic may choose UDP when late data is less useful than lost data. Application protocols can add reliability over UDP.

Study-note section NET21

HTTP defines web request/response semantics; it is stateless, and a message body may be absent. HTTPS adds TLS protection. FTP transfers files using control and separate data connections; it is not the same protocol as SFTP. SMTP submits and relays mail; POP3 retrieves messages and IMAP accesses/synchronizes server mailboxes. Saying SMTP handles both sending and end-user mailbox retrieval is inaccurate.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 18 | lines 9-21

TCP - Transmission Control Protocol: TCP is a reliable connection-oriented, reliable protocol. i.e. a connection is established between the sender and receiver before the data can be transmitted. It divides the data it receives from the upper layer into segments and tags a sequence number to each segment which is used at the receiving end for reordering of data.
UDP - User Datagram Protocol: UDP is a simple protocol used for process to process transmission. It is an unreliable, connectionless protocol for applications that do not require flow control or error control. It simply adds port address, checksum and length information to the data it receives from the upper layer.

Data Communication and Computer Networking module | PDF page 18 | lines 27-32

Application Layer
The Application Layer is a combination of Session, Presentation & Application Layers of OSI models and defines high level protocols like File Transfer (FTP), Electronic Mail (SMTP), Virtual Terminal (TELNET), Domain Name Service (DNS), etc.

Question sources

Computer Science MCQ practice collection · Question 482

Question 180 | AM0483

Which listed devices ordinarily forward frames at OSI layer 2? Select all that apply.

A. Hub

B. Switch

C. Router

D. Bridge

Hint

Match the requested scope or data unit to the layer duties in the note; distinguish hop delivery from end-to-end process delivery.

Answer B, D: Switch; Bridge

A bridge and an ordinary Ethernet switch both inspect link-layer frames and use MAC-address information in forwarding. A hub regenerates and repeats physical signals without that address inspection. A router forwards IP packets between networks using network-layer destinations. The explicit multiple-selection instruction preserves both correct layer-2 devices and avoids implying that only one kind of device can operate at a layer.

Why each choice is right or wrong

A - Incorrect: A hub repeats layer-1 signals rather than making MAC/frame forwarding decisions.

B - Correct: An ordinary Ethernet switch is explicitly a layer-2 forwarding device.

C - Incorrect: A router's defining forwarding function is network-layer IP routing.

D - Correct: A bridge is explicitly a layer-2 device, like an ordinary Ethernet switch.

Primary note proof

Study-note section NET10

> A bridge or ordinary Ethernet switch operates at layer 2. It learns source-MAC-to-port mappings, looks up the destination, forwards a known unicast to its port, filters it if the destination is on the incoming segment, and floods an unknown unicast or broadcast within its VLAN. A switch does not always send only to one destination port. Wireless access points normally bridge wireless and wired link-layer traffic.

Study-note section NET09

> A repeater regenerates layer-1 signals without inspecting destination addresses. An active hub is a multiport repeater: it repeats incoming signals onto other ports, placing half-duplex endpoints in one collision domain. A passive hub is a connector. A hub neither learns MAC addresses nor eliminates collisions. An endpoint such as a network printer consumes services; routers, hubs and access points are intermediary devices.

Study-note section NET11

> Routers forward IP packets between networks using destination prefixes and next hops. They separate broadcast domains and normally do not forward local link broadcasts. A default gateway is usually a router, while a protocol gateway can translate application formats; therefore a gateway is not inherently a device that implements every OSI layer.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 12 | lines 27-37

> SWITCH: A switch filters and forwards data packets
> across anetwork.

Unlike a hub which simply replicates what it receives on oneport onto all the other ports, a switch keeps a record of the MAC addresses of the devices attached to it. When the switch receives a data packet, it forwards the packetdirectly to the recipient device by looking up the MAC address.
• Switch is intelligent and expensive than Hub
• Switch is a point to point communication device
• Hub is a broadcasting device

Data Communication and Computer Networking module | PDF page 12 | lines 60-61

BRIDGE: Connects two LANS having the same protocol - (e.g. Ethernet or Token ring).

Data Communication and Computer Networking module | PDF page 13 | lines 2-8

Filters content by reading the MAC addresses of source and destination.
• MAC to Segment number table
• Do not filter broadcast
• Data not destined for other network is prevented from passing over the bridge
• Slower than repeater due to filtering

Data Communication and Computer Networking module | PDF page 15 | lines 13-40

Data Link Layer
• The Data Link layer adds reliability to the physical layer by providing error detection and correction mechanisms.
• Framing: the Data Link layer receives the data from Network Layer and divides the stream of bits into fixed size manageable units called as Frames and sends it to the physical layer. On the receiver side, the data link layer receives the stream of bits from the physical layer and regroups them into frames and sends them to the Network layer.
• Physical Addressing: The Data link layer appends the physical address in the header of the frame before sending it to physical layer.
• Flow control: The data link layer makes sure that the sender sends the data at a speed at which the receiver canreceive it else if there is an overflow at the receiver sidethe data will be lost.
• Error Control: The data link layer imposes error control mechanism to identify lost or damaged frames, duplicateframes and then retransmit them.
• Access Control: The data link layer imposes

access control mechanism to determine which device has right to send data in an multipoint connection setting.
• Main Responsibility: The main responsibility of the data link layer is hop to hop transmission of frames.

Data Communication and Computer Networking module | PDF page 12 | lines 17-26

Active Hubs
An active hub is actually a multipart repeater. It is normallyused to create connections between stations in a physical startopology.
HUB: Hubs are commonly used to connect segments (devices)of a LAN. Hubs don‘t filter information; instead broadcast incoming packets to all computers connected to it. A hub contains multiple ports which support 8, 12 or 24 RJ-45 ports. Two types: Passive hub and Active hub. It is used in star or ring topology.

Data Communication and Computer Networking module | PDF page 12 | lines 38-52

ROUTER: Router is a specialized network device used tointerconnect different types of network that uses different protocol.
Router allows the users to connect several LAN and WAN
• A LAN to another LAN
• A WAN to another WAN
• A LAN to the Internet
Routers use the routing table to determine how to forwardpackets.
• The list of routing tables provides directions to transfer the data to a particular network destination -various paths to forward the data.
• A router analyzes a destination IP address of a givenpacket and compares it with the routing table to decide the packet's next best path

Question sources

Computer Science MCQ practice collection · Question 483

Question 181 | AM0485

What is the function of a router in a computer network?

A. To connect multiple networks together

B. To amplify the strength of network signals

C. To provide firewall protection

D. To manage network resources and allocate bandwidth

Hint

Compare signal repetition, frame forwarding, packet routing and policy enforcement using the stated device or traffic assumptions.

Answer A: To connect multiple networks together

The router definition explicitly interconnects LANs/WANs and determines next paths using routing tables. Firewall functionality may be added, but it is not the primary definition. Evidence: PDF 12, 11, 48.

Why each choice is right or wrong

A - Correct: Connecting networks is the explicit router role (PDF 12, 11, 48.)

B - Incorrect: Signal regeneration is repeater work (PDF 12, 11, 48.)

C - Incorrect: A router can have firewall configuration, but this is optional additional policy (PDF 12, 11, 48.)

D - Incorrect: Bandwidth allocation is not the defining routing role (PDF 12, 11, 48.)

Primary note proof

Study-note section NET11

> Routers forward IP packets between networks using destination prefixes and next hops. They separate broadcast domains and normally do not forward local link broadcasts. A default gateway is usually a router, while a protocol gateway can translate application formats; therefore a gateway is not inherently a device that implements every OSI layer.

Study-note section NET11

> A firewall allows, rejects or inspects traffic under a security policy; it does not necessarily encrypt. A VPN, Virtual Private Network, provides a logical private connection over another network; a secure VPN authenticates/encrypts its tunnel. A modem modulates outgoing and demodulates incoming carrier signals. These functions may coexist in one home router but remain conceptually distinct.

Study-note section NET09

> A repeater regenerates layer-1 signals without inspecting destination addresses. An active hub is a multiport repeater: it repeats incoming signals onto other ports, placing half-duplex endpoints in one collision domain. A passive hub is a connector. A hub neither learns MAC addresses nor

eliminates collisions. An endpoint such as a network printer consumes services; routers, hubs and access points are intermediary devices.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 12 | lines 38-52

ROUTER: Router is a specialized network device
used tointerconnect different types of network that
uses different protocol.
Router allows the users to connect several LAN and WAN
• A LAN to another LAN
• A WAN to another WAN
• A LAN to the Internet
Routers use the routing table to determine how to
forwardpackets.
• The list of routing tables provides directions to
transfer the data to a particular network
destination -various paths to forward the data.
• A router analyzes a destination IP address of a
givenpacket and compares it with the routing
table to decide the packet's next best path

Data Communication and Computer Networking module | PDF page 11 | lines 54-55

Repeater: A repeater is a device that operates only in the physical
layer. A repeater receives a signal and, before it

Data Communication and Computer Networking module | PDF page 48 | lines 29-40

Network Address Translation (NAT)
NAT translates the IP addresses of computers in a local
network to a single IP address. This address is often used
by the router that connects the computers to the Internet.
The router can be connected to a DSL modem, cable
modem, T1 line, or even a dial-up modem. When other
computers on the Internet attempt to access computers
within the local network, they only see the IP address of
the router. This adds an extra level of security, since the
router can be configured as a firewall, only allowing
authorized systems to access the computers within the
network.

Question sources

Computer Science MCQ practice collection · Question 485

Question 182 | AM0486

Which of the following is a network device that operates at the Physical layer of the OSI model?

A. Switch

B. Hub

C. Router

D. Bridge

Hint

Match the requested scope or data unit to the layer duties in the note; distinguish hop delivery from end-to-end process delivery.

Answer B: Hub

An active hub is explicitly a multiport repeater, and repeaters operate at physical layer. Evidence: PDF 12, 11, 12, 12, 12.

Why each choice is right or wrong

A - Incorrect: Switch forwards by MAC at data-link scope (PDF 12, 11, 12, 12, 12.)

B - Correct: Active hub repeats physical signals (PDF 12, 11, 12, 12, 12.)

C - Incorrect: Router selects IP paths (PDF 12, 11, 12, 12, 12.)

D - Incorrect: Bridge filters by MAC (PDF 12, 11, 12, 12, 12.)

Primary note proof

Study-note section NET09

> A repeater regenerates layer-1 signals without inspecting destination addresses. An active hub is a multiport repeater: it repeats incoming signals onto other ports, placing half-duplex endpoints in one collision domain. A passive hub is a connector. A hub neither learns MAC addresses nor eliminates collisions. An endpoint such as a network printer consumes services; routers, hubs and access points are intermediary devices.

Study-note section NET10

> A bridge or ordinary Ethernet switch operates at layer 2. It learns source-MAC-to-port mappings, looks up the destination, forwards a known unicast to its port, filters it if the destination is on the incoming segment, and floods an unknown unicast or broadcast within its VLAN. A switch does not always send only to one destination port. Wireless access points normally bridge wireless and wired link-layer traffic.

Study-note section NET11

> Routers forward IP packets between networks using destination prefixes and next hops. They separate broadcast domains and normally do not forward local link broadcasts. A default gateway is usually a router, while a protocol gateway can translate application formats; therefore a gateway is not inherently a device that implements every OSI layer.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 12 | lines 17-26

Active Hubs
An active hub is actually a multipart repeater. It is normallyused to create connections between stations in a physical startopology.
HUB: Hubs are commonly used to connect segments (devices)of a LAN. Hubs don‘t filter information; instead broadcast incoming packets to all computers connected to it. A hub contains multiple ports which support 8, 12 or 24 RJ-45 ports. Two types: Passive hub and Active hub. It is used in star or ring topology.

Data Communication and Computer Networking module | PDF page 11 | lines 54-55

Repeater: A repeater is a device that operates only in the physical layer. A repeater receives a signal and, before it

Data Communication and Computer Networking module | PDF page 12 | lines 27-37

SWITCH: A switch filters and forwards data packets across anetwork.
Unlike a hub which simply replicates what it receives on oneport onto all the other ports, a switch keeps a record of the MAC addresses of the devices attached to it.
When the switch receives a data packet, it forwards the packetdirectly to the recipient device by looking up the MAC address.
• Switch is intelligent and expensive than Hub
• Switch is a point to point communication device
• Hub is a broadcasting device

Data Communication and Computer Networking module | PDF page 12 | lines 38-52

ROUTER: Router is a specialized network device used tointerconnect different types of network that uses different protocol.
Router allows the users to connect several LAN and WAN
• A LAN to another LAN
• A WAN to another WAN
• A LAN to the Internet
Routers use the routing table to determine how to forwardpackets.
• The list of routing tables provides directions to transfer the data to a particular network destination -various paths to forward the data.
• A router analyzes a destination IP address of a

givenpacket and compares it with the routing
table to decide the packet's next best path

Data Communication and Computer Networking module | PDF page 12 | lines 60-61

BRIDGE: Connects two LANS having the same protocol -
(e.g. Ethernet or Token ring).

Question sources

Computer Science MCQ practice collection · Question 486

Question 183 | AM0487

Which network component is responsible for converting digital data into analog signals for transmission over telephone lines?

A. Modem

B. Router

C. Switch

D. Firewall

Hint

Compare the signal mechanism, medium properties or transmission direction against the definitions and stated physical assumptions.

Answer A: Modem

The stem asks about conversion for a telephone-line carrier, which is modem modulation. NET11 separates this signal-conversion function from routing IP packets, switching link frames and applying firewall traffic policy. These functions can coexist in one appliance, but the functional component asked for remains the modem.

Why each choice is right or wrong

A - Correct: A modem modulates outgoing carrier signals and demodulates incoming ones, supplying the requested conversion.

B - Incorrect: A router selects next hops between networks; that role is distinct from telephone-carrier modulation.

C - Incorrect: A switch forwards link-layer frames and is not the component defined by carrier modulation.

D - Incorrect: A firewall applies security policy to traffic rather than converting data onto a telephone-line carrier.

Primary note proof

Study-note section NET11

A firewall allows, rejects or inspects traffic under a security policy; it does not necessarily encrypt. A VPN, Virtual Private Network, provides a logical private connection over another network; a secure VPN authenticates/encrypts its tunnel. A modem modulates outgoing and demodulates incoming carrier signals. These functions may coexist in one home router but remain conceptually distinct.

Study-note section NET10

A bridge or ordinary Ethernet switch operates at layer 2. It learns source-MAC-to-port mappings, looks up the destination, forwards a known unicast to its port, filters it if the destination is on the incoming segment, and floods an unknown unicast or broadcast within its VLAN. A switch does not always send only to one destination port. Wireless access points normally bridge wireless and wired link-layer traffic.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 13 | lines 65-77

• Digital modulation is used to convert digital data to analog signal. Ex ASK, FSK, PSK.
Analog Modulation can be accomplished in three ways:
• Amplitude modulation (AM)
• Frequency modulation (FM)
• Phase modulation (PM).
Digital Modulation Types (Digital to Analog signal conversion)
Digital modulation is used to convert digital data to analog signal. It can be accomplished in the following ways:
• Amplitude Shift Keying(ASK)
• Frequency Shift keying (FSK)
• Phase Shift keying (PSK)

Data Communication and Computer Networking module | PDF page 14 | lines 32-49

Physical Layer:
• The Physical Layer provides a standardized interface to physical transmission media, including: Mechanical specification of electrical connectors and cables, for example maximum cable length, Electrical specification of transmission line and Bit-by-bit or symbol-by-symbol delivery.
• Interface: The Physical Layer defines the characteristics of interfaces between the devices & transmission medium.
• Representation of bits: The physical layer is concerned with transmission of signals from one device to another which involves converting data (1_s & 0_s) into signals and vice versa. It is not concerned with the meaning or interpretation of bits.
• Data rate: The physical layer defines the data

transmission rate i.e. number of bits sent per second. It is the responsibility of the physical layer to maintain the defined data rate.

Question sources

Computer Science MCQ practice collection · Question 487

Question 184 | AM0488

Which protocol submits and relays email messages, including acceptance by a receiving mail server? Select one.

A. SMTP

B. HTTP

C. FTP

D. DNS

Hint

Identify the requested service or delivery guarantee, then distinguish application roles, transport behavior and address configuration.

Answer A: SMTP

SMTP is used for mail submission and relay, including a mail server accepting an incoming message. End-user access to stored mail is a separate operation supplied by POP3 or IMAP. HTTP handles web exchanges, FTP transfers files, and DNS resolves records. Specifying server receipt and relay makes the mail-system role clear without assigning mailbox retrieval to the transfer protocol.

Why each choice is right or wrong

A - Correct: SMTP submits and relays mail, including server acceptance of incoming messages.

B - Incorrect: HTTP defines web request/response exchanges rather than the mail submission and relay protocol requested.

C - Incorrect: FTP transfers files and is not the mail submission/relay or mailbox access protocol in the note.

D - Incorrect: DNS resolves records; it does not transport or retrieve the user’s messages.

Primary note proof

Study-note section NET21

HTTP defines web request/response semantics; it is stateless, and a message body may be absent. HTTPS adds TLS protection. FTP transfers files using control and separate data connections; it is not the same protocol as SFTP. SMTP submits and relays mail; POP3 retrieves messages and

IMAP accesses/synchronizes server mailboxes. Saying SMTP handles both sending and end-user mailbox retrieval is inaccurate.

Study-note section NET20

DNS resolves names to records, including IPv4 A and IPv6 AAAA addresses; it can use UDP or TCP port 53. DHCP dynamically leases IPv4 settings, commonly address, mask, gateway and DNS server. Its basic exchange is discover, offer, request, acknowledge. IP itself does not assign addresses.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 28 | lines 32-45

Application Layer
The application layer in TCP/IP is equivalent to the combined session, presentation, and application layers in the OSI model and many protocols are defined at this layer.
The Process/Application Layer Protocols
• Telnet
• File Transfer Protocol (FTP)
• Network File System (NFS).
• Simple Mail Transfer Protocol (SMTP
• POP3 is used to receive mail.
• Simple Network Management Protocol (SNMP)
• Domain Name Service (DNS)
• Dynamic Host Configuration Protocol (DHCP)

Data Communication and Computer Networking module | PDF page 18 | lines 27-32

Application Layer
The Application Layer is a combination of Session, Presentation & Application Layers of OSI models and defines high level protocols like File Transfer (FTP), Electronic Mail (SMTP), Virtual Terminal (TELNET), Domain Name Service (DNS), etc.

Question sources

Computer Science MCQ practice collection · Question 488

Question 185 | AM0489

What is the purpose of DNS (Domain Name System) in computer networks?

A. To encrypt network traffic for secure communication

B. To manage network resources and allocate bandwidth

C. To convert domain names into IP addresses

D. To provide firewall protection

Hint

Identify the requested service or delivery guarantee, then distinguish application roles, transport behavior and address configuration.

Answer C: To convert domain names into IP addresses

The domain naming service is contrasted with explicit host-address entries, supporting resolving a name into the corresponding address. Evidence: PDF 18, 65.

Why each choice is right or wrong

A - Incorrect: Encryption is not DNS naming (PDF 18, 65.)

B - Incorrect: Bandwidth allocation is not DNS naming (PDF 18, 65.)

C - Correct: Name-to-address resolution matches Domain Name Service and the hosts-file contrast (PDF 18, 65.)

D - Incorrect: Firewall access policy is not DNS naming (PDF 18, 65.)

Primary note proof

Study-note section NET20

> DNS resolves names to records, including IPv4 A and IPv6 AAAA addresses; it can use UDP or TCP port 53. DHCP dynamically leases IPv4 settings, commonly address, mask, gateway and DNS server. Its basic exchange is discover, offer, request, acknowledge. IP itself does not assign addresses.

Study-note section NET11

> A firewall allows, rejects or inspects traffic under a security policy; it does not necessarily encrypt. A VPN, Virtual Private Network, provides a logical private connection over another network; a secure VPN authenticates/encrypts its tunnel. A modem modulates outgoing and demodulates incoming carrier signals. These functions may coexist in one home router but remain conceptually distinct.

Study-note section NET-S02

> Quality of service (QoS) controls traffic treatment to meet objectives such as throughput, delay, jitter or loss. Classification, queue scheduling and allocation of buffer or bandwidth resources implement such treatment. QoS concerns delivered service behavior; scalability concerns accommodating growth, and security concerns unauthorized actions.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 18 | lines 27-32

> Application Layer
> The Application Layer is a combination of Session,
> Presentation & Application Layers of OSI models and defines
> high level protocols like File Transfer (FTP), Electronic Mail
> (SMTP), Virtual Terminal (TELNET), Domain Name Service
> (DNS), etc.

Data Communication and Computer Networking module | PDF page 65 | lines 31-38

> /etc/hosts
> The /etc/hosts file always contains the localhost IP
> address, 127.0.0.1, which is
> usedfor interprocess communication.
> Never remove this line! Sometimes contains
> addresses of additional hosts, whichcan be contacted
> without using an external naming service such as
> DNS (the Domain Name Server).

Question sources

Computer Science MCQ practice collection · Question 489

Question 186 | AM0490

Which listed application protocol has the name File Transfer Protocol?

A. HTTP

B. FTP

C. SMTP

D. TCP

Hint

Identify the requested service or delivery guarantee, then distinguish application roles, transport behavior and address configuration.

Answer B: FTP

FTP is the named application protocol File Transfer Protocol. HTTP also transfers resource bodies and can download files, so generic file transfer alone does not distinguish them. SMTP is a mail-transfer application protocol, while TCP supplies an underlying reliable byte-stream transport. The explicit protocol name identifies the intended service without claiming that FTP is the only way to transfer a file.

Why each choice is right or wrong

A - Incorrect: HTTP is Hypertext Transfer Protocol and can carry files, but is not the stated protocol name.

B - Correct: FTP expands to File Transfer Protocol.

C - Incorrect: SMTP sends and relays email rather than bearing the stated protocol name.

D - Incorrect: TCP is a transport protocol, not the named application protocol.

Primary note proof

Study-note section NET21

HTTP defines web request/response semantics; it is stateless, and a message body may be absent. HTTPS adds TLS protection. FTP transfers files using control and separate data connections; it is not the same protocol as SFTP. SMTP submits and relays mail; POP3 retrieves messages and IMAP accesses/synchronizes server mailboxes. Saying SMTP handles both sending and end-user mailbox retrieval is inaccurate.

Study-note section NET17

TCP offers a reliable ordered byte stream using sequence numbers, acknowledgments, retransmission and windows. Flow control protects the receiver; congestion control protects network capacity. UDP sends independent datagrams with ports and a checksum but no built-in setup, delivery guarantee, retransmission or ordering. Live interactive traffic may choose UDP when late data is less useful than lost data. Application protocols can add reliability over UDP.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 18 | lines 27-32

Application Layer
The Application Layer is a combination of Session,
Presentation & Application Layers of OSI models and defines
high level protocols like File Transfer (FTP), Electronic Mail
(SMTP), Virtual Terminal (TELNET), Domain Name Service
(DNS), etc.

Data Communication and Computer Networking module | PDF page 28 | lines 32-45

Application Layer
The application layer in TCP/IP is equivalent to the
combined session, presentation, and application layers in
the OSI model and many protocols are defined at this
layer.
The Process/Application Layer Protocols
• Telnet
• File Transfer Protocol (FTP)
• Network File System (NFS).
• Simple Mail Transfer Protocol (SMTP
• POP3 is used to receive mail.

• Simple Network Management Protocol (SNMP)
• Domain Name Service (DNS)
• Dynamic Host Configuration Protocol (DHCP)

Data Communication and Computer Networking module | PDF page 18 | lines 9-21

TCP - Transmission Control Protocol: TCP is a reliable connection-oriented, reliable protocol. i.e. a connection is established between the sender and receiver before the data can be transmitted. It divides the data it receives from the upper layer into segments and tags a sequence number to each segment which is used at the receiving end for reordering of data.
UDP - User Datagram Protocol: UDP is a simple protocol used for process to process transmission. It is an unreliable, connectionless protocol for applications that do not require flow control or error control. It simply adds port address, checksum and length information to the data it receives from the upper layer.

Question sources

Computer Science MCQ practice collection · Question 490

Question 187 | AM0491

Which device connects multiple Ethernet LAN endpoints and learns MAC-to-port mappings to forward known unicast frames selectively?

A. Hub

B. Router

C. Switch

D. Modem

Hint

Compare signal repetition, frame forwarding, packet routing and policy enforcement using the stated device or traffic assumptions.

Answer C: Switch

Both hubs and switches can connect LAN endpoints, but their forwarding behavior differs. A hub repeats incoming signals to its other ports without learning addresses. An ordinary Ethernet switch learns source MAC-to-port mappings and uses the destination MAC address to forward known unicasts. Routers instead forward IP packets between networks, while modems convert carrier signals. The added forwarding requirement distinguishes the intended device.

Why each choice is right or wrong

A - Incorrect: A hub connects endpoints but repeats signals without learning MAC-to-port mappings.

B - Incorrect: A router's defining function is connecting/routing between IP networks rather than this shared LAN-device role.

C - Correct: A switch learns MAC-to-port mappings and forwards known unicasts selectively.

D - Incorrect: A modem modulates/demodulates carrier signals rather than providing the offered multiport LAN interconnection function.

Primary note proof

Study-note section NET10

> A bridge or ordinary Ethernet switch operates at layer 2. It learns source-MAC-to-port mappings, looks up the destination, forwards a known unicast to its port, filters it if the destination is on the incoming segment, and floods an unknown unicast or broadcast within its VLAN. A switch does not always send only to one destination port. Wireless access points normally bridge wireless and wired link-layer traffic.

Study-note section NET09

> A repeater regenerates layer-1 signals without inspecting destination addresses. An active hub is a multiport repeater: it repeats incoming signals onto other ports, placing half-duplex endpoints in one collision domain. A passive hub is a connector. A hub neither learns MAC addresses nor eliminates collisions. An endpoint such as a network printer consumes services; routers, hubs and access points are intermediary devices.

Study-note section NET11

> A firewall allows, rejects or inspects traffic under a security policy; it does not necessarily encrypt. A VPN, Virtual Private Network, provides a logical private connection over another network; a secure VPN authenticates/encrypts its tunnel. A modem modulates outgoing and demodulates incoming carrier signals. These functions may coexist in one home router but remain conceptually distinct.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 12 | lines 17-26

> Active Hubs
> An active hub is actually a multipart repeater. It is normallyused to create connections between stations in a physical startopology.
> HUB: Hubs are commonly used to connect segments (devices)of a LAN. Hubs don‘t filter information; instead broadcast incoming packets to all computers connected to it. A hub contains multiple ports which support 8, 12 or 24 RJ-45 ports. Two types: Passive hub and Active hub. It is used in star or ring topology.

Data Communication and Computer Networking module | PDF page 12 | lines 27-37

SWITCH: A switch filters and forwards data packets across anetwork.
Unlike a hub which simply replicates what it receives on oneport onto all the other ports, a switch keeps a record of the MAC addresses of the devices attached to it.
When the switch receives a data packet, it forwards the packetdirectly to the recipient device by looking up the MAC address.
• Switch is intelligent and expensive than Hub
• Switch is a point to point communication device
• Hub is a broadcasting device

Data Communication and Computer Networking module | PDF page 22 | lines 26-44

Personal Area Network (PAN): is a network may be spanned across a given table with distances between the devices not more than few meters. The technology used to interconnect the devices could be a Bluetooth. These networks are called Personal Area Networks, since the devices interconnected in these networks are belongs to a single person.
Local Area Network (LAN): is a network that may span across a building, or across several buildings within a single organization, by using intermediate devices, like switches and/or hubs, to interconnect devices in all floors.
Metropolitan Area Network (MAN): is a network that may span across a whole city interconnecting several buildings and organizations.
Wide Area Network (WAN): is a network that may span across multiple cities, or an entire country, or an entire continent or it may even cover the whole world. For example, an Internet is one example of WAN.

Question sources

Computer Science MCQ practice collection · Question 491

Question 188 | AM0492

What is the primary function of a firewall in a computer network?

A. To manage network resources and allocate bandwidth

B. To encrypt network traffic for secure communication

C. To filter and monitor network traffic for security purposes

D. To convert domain names into IP addresses

Hint

Use the cited note definitions to identify the requested function or scope, then check each alternative against that same rule.

Answer C: To filter and monitor network traffic for security purposes

The firewall example controls which systems may access internal computers; monitoring/filtering for security is the offered match. Evidence: PDF 48, 16, 18.

Why each choice is right or wrong

A - Incorrect: Resource/bandwidth allocation is not the described firewall role (PDF 48, 16, 18.)

B - Incorrect: Encryption is a presentation function and distinct from access filtering (PDF 48, 16, 18.)

C - Correct: Authorized-access filtering is the module firewall function (PDF 48, 16, 18.)

D - Incorrect: DNS is the naming service, not firewall policy (PDF 48, 16, 18.)

Primary note proof

Study-note section NET11

> A firewall allows, rejects or inspects traffic under a security policy; it does not necessarily encrypt. A VPN, Virtual Private Network, provides a logical private connection over another network; a secure VPN authenticates/encrypts its tunnel. A modem modulates outgoing and demodulates incoming carrier signals. These functions may coexist in one home router but remain conceptually distinct.

Study-note section NET-S02

> Quality of service (QoS) controls traffic treatment to meet objectives such as throughput, delay, jitter or loss. Classification, queue scheduling and allocation of buffer or bandwidth resources implement such treatment. QoS concerns delivered service behavior; scalability concerns accommodating growth, and security concerns unauthorized actions.

Study-note section NET20

> DNS resolves names to records, including IPv4 A and IPv6 AAAA addresses; it can use UDP or TCP port 53. DHCP dynamically leases IPv4 settings, commonly address, mask, gateway and DNS server. Its basic exchange is discover, offer, request, acknowledge. IP itself does not assign addresses.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 48 | lines 29-40

> Network Address Translation (NAT)
> NAT translates the IP addresses of computers in a local
> network to a single IP address. This address is often used
> by the router that connects the computers to the Internet.
> The router can be connected to a DSL modem, cable

modem, T1 line, or even a dial-up modem. When other computers on the Internet attempt to access computers within the local network, they only see the IP address of the router. This adds an extra level of security, since the router can be configured as a firewall, only allowing authorized systems to access the computers within the network.

Data Communication and Computer Networking module | PDF page 16 | lines 33-42

Presentation Layer
• The communicating devices may be having different platforms. The presentation layer performs translation, encryption and compression of data.
• The presentation layer receives the data from the application layer adds header which contains information related to encryption and compression and sends it to the session layer.
• So, the main responsibility of the Presentation layer is translation, compression and encryption.

Data Communication and Computer Networking module | PDF page 18 | lines 27-32

Application Layer
The Application Layer is a combination of Session, Presentation & Application Layers of OSI models and defines high level protocols like File Transfer (FTP), Electronic Mail (SMTP), Virtual Terminal (TELNET), Domain Name Service (DNS), etc.

Question sources

Computer Science MCQ practice collection · Question 492

Question 189 | AM0493

Which protocol is responsible for assigning IP addresses to devices on a network automatically?

A. HTTP

B. DNS

C. DHCP

D. FTP

Hint

Compare signal repetition, frame forwarding, packet routing and policy enforcement using the stated device or traffic assumptions.

Answer C: DHCP

NET20 assigns dynamic address-setting leases to DHCP, whose basic exchange is discover, offer, request and acknowledge. DNS instead resolves names to records. HTTP and FTP are application services for web exchanges and file transfer; neither is the automatic host-address lease protocol.

Why each choice is right or wrong

A - Incorrect: HTTP provides web request/response semantics rather than automatic IP-address leases.

B - Incorrect: DNS resolves names into records, including addresses, but does not lease the host's own address.

C - Correct: DHCP dynamically leases an IP address and related host-network configuration.

D - Incorrect: FTP transfers files; it does not provide the address-assignment exchange described.

Primary note proof

Study-note section NET20

> DNS resolves names to records, including IPv4 A and IPv6 AAAA addresses; it can use UDP or TCP port 53. DHCP dynamically leases IPv4 settings, commonly address, mask, gateway and DNS server. Its basic exchange is discover, offer, request, acknowledge. IP itself does not assign addresses.

Study-note section NET21

> HTTP defines web request/response semantics; it is stateless, and a message body may be absent. HTTPS adds TLS protection. FTP transfers files using control and separate data connections; it is not the same protocol as SFTP. SMTP submits and relays mail; POP3 retrieves messages and IMAP accesses/synchronizes server mailboxes. Saying SMTP handles both sending and end-user mailbox retrieval is inaccurate.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 28 | lines 32-45

> Application Layer
> The application layer in TCP/IP is equivalent to the
> combined session, presentation, and application layers in
> the OSI model and many protocols are defined at this
> layer.
> The Process/Application Layer Protocols
> • Telnet
> • File Transfer Protocol (FTP)
> • Network File System (NFS).
> • Simple Mail Transfer Protocol (SMTP
> • POP3 is used to receive mail.
> • Simple Network Management Protocol (SNMP)

• Domain Name Service (DNS)
• Dynamic Host Configuration Protocol (DHCP)

Question sources

Computer Science MCQ practice collection · Question 493

Question 190 | AM0494

Which OSI layer establishes and manages application dialogs, including checkpoints for recovery after an interruption?

A. Physical layer

B. Data Link layer

C. Transport layer

D. Session layer

Hint

Match the requested scope or data unit to the layer duties in the note; distinguish hop delivery from end-to-end process delivery.

Answer D: Session layer

Session-layer roles include establishing and managing dialogs and coordinating checkpoints so a transfer can resume after an interruption. TCP transport connections are a different form of connection state and do not make every reference to a dialog a transport function. Physical signaling and hop-local link delivery likewise have different scopes. The revised stem identifies dialog and checkpoint management as the lifecycle being classified.

Why each choice is right or wrong

A - Incorrect: Physical signaling does not perform application-dialog management or checkpoint coordination.

B - Incorrect: Data link handles hop-local frames and link procedures rather than application dialogs and checkpoints.

C - Incorrect: Transport handles process delivery and TCP connection state, not the session-dialog role specified.

D - Correct: Session manages dialogs and can coordinate checkpoints for recovery.

Primary note proof

Study-note section NET19

OSI session roles establish/manage dialogs and can coordinate checkpoints so transfer resumes after interruption. Presentation roles translate encodings and handle compression/encryption. Compression reduces representation size; encryption hides content and need not shrink it. Application protocols provide services directly to applications. Practical implementations

distribute these functions differently; TLS is not proof of a separate physical presentation-layer device.

Study-note section NET18

TCP establishes state with SYN, SYN+ACK, then ACK. SYN consumes one sequence position even with no application bytes. An acknowledgment states the next expected sequence number. For client ISN=395 and server ISN=260: client sends SYN seq395; server sends SYN+ACK seq260 ack396; client sends ACK seq396 ack261. Later byte counts advance sequence numbers. FIN also consumes one sequence position.

Study-note section NET14

Controlled access uses polling, reservations or a token to grant turns; correctly coordinated access avoids contention collisions. Channelization divides frequency, time or code resources. Stop-and-wait sends one frame and waits for ACK, retransmitting on timeout; sequence bits distinguish duplicates. Sliding windows permit multiple unacknowledged frames. Link reliability/flow control is hop-local; transport reliability/flow control is end-to-end. Ethernet detects corruption but does not itself guarantee reliable delivery.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 16 | lines 18-32

Session Layer
• The session layer establishes a session between the communicating devices called dialog and synchronizes their interaction. It is the responsibility of the session layer to establish and synchronize the dialogs. It is also called the network dialog controller.
• The session layer at the sending side accepts data from the presentation layer adds checkpoints to it called sync bits and passes the data to the transport layer. At the receiving end the session layer receives data from the transport layer removes the checkpoints inserted previously and passes the data to the presentation layer. So, the main responsibility of session layer is dialog control and synchronization.

Data Communication and Computer Networking module | PDF page 16 | lines 2-17

• At the sending side, the transport layer receives data from the session layer, divides it into units called segments and sends it to the network layer.
• To ensure process to process delivery the transport layer makes use of port address to identify the data from the sending and receiving process.
• The data can be transported in a connection oriented or connectionless manner.

• The Transport layer is responsible for segmentation and reassembly of the message into segments which bear sequence numbers.
• The transport layer also carries out flow control and error control functions; but unlike data link layer these are end to end rather than node to node.
• The main responsibility of the transport layer is process to process delivery of the entire message

Data Communication and Computer Networking module | PDF page 14 | lines 32-49

Physical Layer:
• The Physical Layer provides a standardized interface to physical transmission media, including: Mechanical specification of electrical connectors and cables, for example maximum cable length, Electrical specification of transmission line and Bit-by-bit or symbol-by-symbol delivery.
• Interface: The Physical Layer defines the characteristics of interfaces between the devices & transmission medium.
• Representation of bits: The physical layer is concerned with transmission of signals from one device to another which involves converting data (1_s & 0_s) into signals and vice versa. It is not concerned with the meaning or interpretation of bits.
• Data rate: The physical layer defines the data transmission rate i.e. number of bits sent per second. It is the responsibility of the physical layer to maintain the defined data rate.

Data Communication and Computer Networking module | PDF page 15 | lines 13-40

Data Link Layer
• The Data Link layer adds reliability to the physical layer by providing error detection and correction mechanisms.
• Framing: the Data Link layer receives the data from Network Layer and divides the stream of bits into fixed size manageable units called as Frames and sends it to the physical layer. On the receiver side, the data link layer receives the stream of bits from the physical layer and regroups them into frames and sends them to the Network layer.
• Physical Addressing: The Data link layer appends the physical address in the header of the frame before sending it to physical layer.
• Flow control: The data link layer makes sure that the sender sends the data at a speed at which the

receiver canreceive it else if there is an overflow at the receiver sidethe data will be lost.
• Error Control: The data link layer imposes error control mechanism to identify lost or damaged frames, duplicateframes and then retransmit them.
• Access Control: The data link layer imposes access control mechanism to determine which device has right to send data in an multipoint connection setting.
• Main Responsibility: The main responsibility of the data link layer is hop to hop transmission of frames.

Question sources

Computer Science MCQ practice collection · Question 494

Question 191 | AM0495

Which protocol is used for reliable data delivery at the transport layer in the TCP/IP protocol suite?

A. UDP

B. IP

C. FTP

D. TCP

Hint

Match the requested scope or data unit to the layer duties in the note; distinguish hop delivery from end-to-end process delivery.

Answer D: TCP

TCP is explicitly reliable and connection-oriented at transport, unlike UDP and network-layer IP. Evidence: PDF 18, 17, 18.

Why each choice is right or wrong

A - Incorrect: UDP is explicitly unreliable (PDF 18, 17, 18.)

B - Incorrect: IP is network-layer best effort (PDF 18, 17, 18.)

C - Incorrect: FTP is application file transfer (PDF 18, 17, 18.)

D - Correct: TCP is the explicitly reliable transport protocol (PDF 18, 17, 18.)

Primary note proof

Study-note section NET17

TCP offers a reliable ordered byte stream using sequence numbers, acknowledgments, retransmission and windows. Flow control protects the receiver; congestion control protects network capacity. UDP sends independent datagrams with ports and a checksum but no built-in setup, delivery guarantee, retransmission or ordering. Live interactive traffic may choose UDP when late data is less useful than lost data. Application protocols can add reliability over UDP.

Study-note section NET16

IP supplies connectionless best-effort packet delivery, not end-to-end ordering or retransmission. IPv4 addresses are 32 bits. Its minimum header is 20 bytes and can grow to 60 bytes; it is not a 32-bit header. IHL counts 32-bit words; total length includes header and payload. TTL limits lifetime across routers; the protocol field identifies TCP, UDP or another upper-layer protocol.

Study-note section NET21

HTTP defines web request/response semantics; it is stateless, and a message body may be absent. HTTPS adds TLS protection. FTP transfers files using control and separate data connections; it is not the same protocol as SFTP. SMTP submits and relays mail; POP3 retrieves messages and IMAP accesses/synchronizes server mailboxes. Saying SMTP handles both sending and end-user mailbox retrieval is inaccurate.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 18 | lines 9-21

TCP - Transmission Control Protocol: TCP is a reliable connection-oriented, reliable protocol. i.e. a connection is established between the sender and receiver before the data can be transmitted. It divides the data it receives from the upper layer into segments and tags a sequence number to each segment which is used at the receiving end for reordering of data.
UDP - User Datagram Protocol: UDP is a simple protocol used for process to process transmission. It is an unreliable, connectionless protocol for applications that do not require flow control or error control. It simply adds port address, checksum and length information to the data it receives from the upper layer.

Data Communication and Computer Networking module | PDF page 17 | lines 22-38

Network Layer or IP
Also called as the Internetwork Layer (IP). It holds the IP protocol which is a network layer protocol and is responsiblefor source to destination transmission of data.
The Internetworking Protocol (IP) is a connection-less & unreliable protocol.
It is a best effort delivery service. i.e. there is no error checking in IP, it simply sends the data and relies on its

underlying layers to get the data transmitted to the destination.Even if it is unreliable IP cannot be considered weak and useless; since it provides only the functionality that is requiredfor transmitting data thereby giving maximum efficiency.
Since there is no mechanism of error detection or correction in IP, there will be no delay introduced on a medium where thereis no error at all.

Data Communication and Computer Networking module | PDF page 18 | lines 27-32

Application Layer
The Application Layer is a combination of Session, Presentation & Application Layers of OSI models and defines high level protocols like File Transfer (FTP), Electronic Mail (SMTP), Virtual Terminal (TELNET), Domain Name Service (DNS), etc.

Question sources

Computer Science MCQ practice collection · Question 495

Question 192 | AM0496

Which layer of the OSI reference model is responsible for addressing and routing data packets across different networks?

A. Network layer

B. Data Link layer

C. Transport layer

D. Physical layer

Hint

Match the requested scope or data unit to the layer duties in the note; distinguish hop delivery from end-to-end process delivery.

Answer A: Network layer

Network explicitly adds logical addressing and routes packets from source to destination across intermediate devices. Evidence: PDF 15, 15, 16, 14.

Why each choice is right or wrong

A - Correct: Network has addressing and routing responsibilities (PDF 15, 15, 16, 14.)

B - Incorrect: Data link handles physical addresses and one-hop frames (PDF 15, 15, 16, 14.)

C - Incorrect: Transport delivers to processes with ports (PDF 15, 15, 16, 14.)

D - Incorrect: Physical delivers bits/signals (PDF 15, 15, 16, 14.)

Primary note proof

Study-note section NET30

Routing computes paths; forwarding chooses a next hop for an individual packet. Select the matching route with the longest prefix, then apply the routing system's tie-breaking criteria. A default /0 matches when nothing more specific does. Static routes are configured; dynamic protocols exchange reachability. Distance vector uses neighbor estimates, while link state distributes link information and computes shortest paths. Interior protocols operate within an autonomous system; BGP exchanges routes between systems.

Study-note section NET12

Sending proceeds from application data to transport segment/datagram, network packet, link frame and physical bits/symbols; receiving reverses the order. Each layer serves the layer above. A router removes a received link frame, inspects IP, and creates a new link frame for the next hop. MAC addresses usually change across routed hops; end-to-end IP addresses ordinarily remain until translation.

Study-note section NET17

Ports identify transport endpoints; the application can choose a transport and request socket buffer sizes, subject to OS limits. A TCP connection is identified by source/destination IP and source/destination port, with TCP understood. IPv4 protocol numbers identify upper protocols; 80 is a usual HTTP port, not an IP protocol number. Clients often use ephemeral ports. SCTP is a reliable message-oriented transport with multiple streams.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 15 | lines 41-61

Network Layer
• The network layer makes sure that the data is deliveredto the receiver despite multiple intermediate devices.
• The network layer at the sending side accepts data from the transport layer, divides it into packets, addsaddressing information in the header and passes it tothe data link layer.
• The network layer is responsible for source todestination of delivery of data.
• The network layer uses logical address commonlyknown as IP address to recognize devices on the network.
• Each packet is independent of the other and may travelusing different routes to reach the receiver hence may arrive out of turn at the receiver (Routing).
• The Network layer does not perform any flow controlor error control

• The main responsibility of Network Layer is transmission of packets from source to destination

Data Communication and Computer Networking module | PDF page 15 | lines 13-40

Data Link Layer
• The Data Link layer adds reliability to the physical layer by providing error detection and correction mechanisms.
• Framing: the Data Link layer receives the data from Network Layer and divides the stream of bits into fixed size manageable units called as Frames and sends it to the physical layer. On the receiver side, the data link layer receives the stream of bits from the physical layer and regroups them into frames and sends them to the Network layer.
• Physical Addressing: The Data link layer appends the physical address in the header of the frame before sending it to physical layer.
• Flow control: The data link layer makes sure that the sender sends the data at a speed at which the receiver canreceive it else if there is an overflow at the receiver sidethe data will be lost.
• Error Control: The data link layer imposes error control mechanism to identify lost or damaged frames, duplicateframes and then retransmit them.
• Access Control: The data link layer imposes access control mechanism to determine which device has right to send data in an multipoint connection setting.
• Main Responsibility: The main responsibility of the data link layer is hop to hop transmission of frames.

Data Communication and Computer Networking module | PDF page 16 | lines 2-17

• At the sending side, the transport layer receives data from the session layer, divides it into units called segments and sends it to the network layer.
• To ensure process to process delivery the transport layer makes use of port address to identify the data from the sending and receiving process.
• The data can be transported in a connection oriented or connectionless manner.
• The Transport layer is responsible for segmentation and reassembly of the message into segments which bear sequence numbers.
• The transport layer also carries out flow control and

error control functions; but unlike data link layer these are end to end rather than node to node.
• The main responsibility of the transport layer is process to process delivery of the entire message

Data Communication and Computer Networking module | PDF page 14 | lines 32-49

Physical Layer:
• The Physical Layer provides a standardized interface to physical transmission media, including: Mechanical specification of electrical connectors and cables, for example maximum cable length, Electrical specification of transmission line and Bit-by-bit or symbol-by-symbol delivery.
• Interface: The Physical Layer defines the characteristics of interfaces between the devices & transmission medium.
• Representation of bits: The physical layer is concerned with transmission of signals from one device to another which involves converting data (1_s & 0_s) into signals and vice versa. It is not concerned with the meaning or interpretation of bits.
• Data rate: The physical layer defines the data transmission rate i.e. number of bits sent per second. It is the responsibility of the physical layer to maintain the defined data rate.

Question sources

Computer Science MCQ practice collection · Question 496

Question 193 | AM0497

Which OSI layer supplies hop-local frame acknowledgments and retransmission when a reliable-link protocol is used, rather than end-to-end transport recovery?

A. Network layer

B. Transport layer

C. Data Link layer

D. Application layer

Hint

Match the requested scope or data unit to the layer duties in the note; distinguish hop delivery from end-to-end process delivery.

Answer C: Data Link layer

Reliable data-link protocols can acknowledge frames and retransmit missing or damaged frames across a single hop. Transport recovery instead covers the end-to-end communication between processes. Network-layer IPv4 includes a header checksum but remains best-effort and does not supply this frame ARQ service. The link-layer role is protocol-dependent: Ethernet error detection alone does not guarantee reliable local delivery.

Why each choice is right or wrong

A - Incorrect: IP routing and its header checksum are not the requested hop-local frame ARQ service.

B - Incorrect: Transport reliability has end-to-end rather than one-link scope.

C - Correct: Data link implements the specified hop-local frame acknowledgment/retransmission procedure.

D - Incorrect: Application services are above the specified link-frame recovery mechanism.

Primary note proof

Study-note section NET14

> Controlled access uses polling, reservations or a token to grant turns; correctly coordinated access avoids contention collisions. Channelization divides frequency, time or code resources. Stop-and-wait sends one frame and waits for ACK, retransmitting on timeout; sequence bits distinguish duplicates. Sliding windows permit multiple unacknowledged frames. Link reliability/flow control is hop-local; transport reliability/flow control is end-to-end. Ethernet detects corruption but does not itself guarantee reliable delivery.

Study-note section NET13

> Detection adds redundancy but does not guarantee correction. Even parity adds a bit so the total number of ones is even: 1011 needs parity 1. It detects every odd number of bit flips but misses even counts. CRC treats bits as a polynomial and appends the XOR-division remainder; the receiver repeats the division. Internet checksums add words with end-around carry and complement the sum. A burst spans from the first corrupted bit through the last, including unchanged interior bits. Retransmission or sufficient forward-error-correcting redundancy is needed for recovery.

Study-note section NET16

> The IPv4 checksum protects its header; IP does not lack error checking altogether. Identification, flags and offset support fragmentation. IPv4 sources and routers may fragment when allowed; reassembly occurs at the destination. If DF is set and the next MTU is too small, forwarding fails and an ICMP diagnostic may be returned.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 15 | lines 13-40

Data Link Layer
• The Data Link layer adds reliability to the physical layer by providing error detection and correction mechanisms.
• Framing: the Data Link layer receives the data from Network Layer and divides the stream of bits into fixed size manageable units called as Frames and sends it to the physical layer. On the receiver side, the data link layer receives the stream of bits from the physical layer and regroups them into frames and sends them to the Network layer.
• Physical Addressing: The Data link layer appends the physical address in the header of the frame before sending it to physical layer.
• Flow control: The data link layer makes sure that the sender sends the data at a speed at which the receiver canreceive it else if there is an overflow at the receiver sidethe data will be lost.
• Error Control: The data link layer imposes error control mechanism to identify lost or damaged frames, duplicateframes and then retransmit them.
• Access Control: The data link layer imposes access control mechanism to determine which device has right to send data in an multipoint connection setting.
• Main Responsibility: The main responsibility of the data link layer is hop to hop transmission of frames.

Data Communication and Computer Networking module | PDF page 16 | lines 2-17

• At the sending side, the transport layer receives data from the session layer, divides it into units called segments and sends it to the network layer.
• To ensure process to process delivery the transport layer makes use of port address to identify the data from the sending and receiving process.
• The data can be transported in a connection oriented or connectionless manner.
• The Transport layer is responsible for segmentation and reassembly of the message into segments which bear sequence numbers.
• The transport layer also carries out flow control and error control functions; but unlike data link layer these are end to end rather than node to node.
• The main responsibility of the transport layer is process to process delivery of the entire message

Data Communication and Computer Networking module | PDF page 15 | lines 41-61

Network Layer
• The network layer makes sure that the data is deliveredto the receiver despite multiple intermediate devices.
• The network layer at the sending side accepts data from the transport layer, divides it into packets, addsaddressing information in the header and passes it tothe data link layer.
• The network layer is responsible for source todestination of delivery of data.
• The network layer uses logical address commonlyknown as IP address to recognize devices on the network.
• Each packet is independent of the other and may travelusing different routes to reach the receiver hence may arrive out of turn at the receiver (Routing).
• The Network layer does not perform any flow controlor error control
• The main responsibility of Network Layer is transmission of packets from source to destination

Data Communication and Computer Networking module | PDF page 16 | lines 43-47

Application Layer
• The application layer enables the user to communicate its data to the receiver by providing certain services.
• The main Responsibility of Application layer is to provide the user access to network resources.

Question sources

Computer Science MCQ practice collection · Question 497

Question 194 | AM0498

Which protocol submits and relays email messages, including acceptance by a receiving mail server? Select one.

A. SMTP

B. FTP

C. HTTP

D. DNS

Hint

Identify the requested service or delivery guarantee, then distinguish application roles, transport behavior and address configuration.

Answer A: SMTP

SMTP is used for mail submission and relay, including a mail server accepting an incoming message. End-user access to stored mail is a separate operation supplied by POP3 or IMAP. HTTP handles web exchanges, FTP transfers files, and DNS resolves records. Specifying server receipt and relay makes the mail-system role clear without assigning mailbox retrieval to the transfer protocol.

Why each choice is right or wrong

A - Correct: SMTP submits and relays mail, including server acceptance of incoming messages.

B - Incorrect: FTP transfers files through a separate protocol rather than the mail flow defined here.

C - Incorrect: HTTP defines web request/response exchanges rather than the mail submission and relay protocol requested.

D - Incorrect: DNS supplies records such as mail-exchanger names rather than delivering or retrieving message contents.

Primary note proof

Study-note section NET21

> HTTP defines web request/response semantics; it is stateless, and a message body may be absent. HTTPS adds TLS protection. FTP transfers files using control and separate data connections; it is not the same protocol as SFTP. SMTP submits and relays mail; POP3 retrieves messages and IMAP accesses/synchronizes server mailboxes. Saying SMTP handles both sending and end-user mailbox retrieval is inaccurate.

Study-note section NET20

> DNS resolves names to records, including IPv4 A and IPv6 AAAA addresses; it can use UDP or TCP port 53. DHCP dynamically leases IPv4 settings, commonly address, mask, gateway and DNS server. Its basic exchange is discover, offer, request, acknowledge. IP itself does not assign addresses.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 28 | lines 32-45

> Application Layer
> The application layer in TCP/IP is equivalent to the
> combined session, presentation, and application layers in
> the OSI model and many protocols are defined at this
> layer.
> The Process/Application Layer Protocols
> • Telnet
> • File Transfer Protocol (FTP)
> • Network File System (NFS).
> • Simple Mail Transfer Protocol (SMTP

• POP3 is used to receive mail.
• Simple Network Management Protocol (SNMP)
• Domain Name Service (DNS)
• Dynamic Host Configuration Protocol (DHCP)

Data Communication and Computer Networking module | PDF page 18 | lines 27-32

Application Layer
The Application Layer is a combination of Session,
Presentation & Application Layers of OSI models and defines
high level protocols like File Transfer (FTP), Electronic Mail
(SMTP), Virtual Terminal (TELNET), Domain Name Service
(DNS), etc.

Question sources

Computer Science MCQ practice collection · Question 498

Question 195 | AM0499

Which layer of the OSI reference model is responsible for converting data into a format suitable for transmission over a network?

A. Presentation layer

B. Session layer

C. Physical layer

D. Application layer

Hint

Match the requested scope or data unit to the layer duties in the note; distinguish hop delivery from end-to-end process delivery.

Answer A: Presentation layer for representation/format translation

The word format identifies representation translation rather than routing or connection management. NET19 assigns encoding translation and other representation work to presentation. Physical signaling maps bits to medium symbols, but does not supply the application-data format translation asked for. Thus A matches the intended formatting responsibility.

Why each choice is right or wrong

A - Correct: Presentation translates representations/encodings into suitable data formats.

B - Incorrect: Session manages dialogs and checkpoints rather than data representation formats.

C - Incorrect: Physical maps bits/symbols to signals, a different responsibility from representation-format translation.

D - Incorrect: Application supplies network services to applications rather than the distinct presentation-format function.

Primary note proof

Study-note section NET19

OSI session roles establish/manage dialogs and can coordinate checkpoints so transfer resumes after interruption. Presentation roles translate encodings and handle compression/encryption. Compression reduces representation size; encryption hides content and need not shrink it. Application protocols provide services directly to applications. Practical implementations distribute these functions differently; TLS is not proof of a separate physical presentation-layer device.

Study-note section NET09

A NIC supplies a computer's network interface and commonly implements both physical and link functions. Calling a NIC a physical interface does not mean all its functions are layer 1. Physical specifications include connectors, signaling, voltage, timing and physical coding/modulation; the PHY interface to MAC handles hardware signaling.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 16 | lines 33-42

Presentation Layer
• The communicating devices may be having different platforms. The presentation layer performs translation, encryption and compression of data.
• The presentation layer receives the data from the application layer adds header which contains information related to encryption and compression and sends it to the session layer.
• So, the main responsibility of the Presentation layer is translation, compression and encryption.

Data Communication and Computer Networking module | PDF page 14 | lines 32-49

Physical Layer:
• The Physical Layer provides a standardized interface to physical transmission media, including: Mechanical specification of electrical connectors and cables, for example maximum cable length, Electrical specification of transmission line and Bit-by-bit or symbol-by-symbol delivery.
• Interface: The Physical Layer defines the characteristics of interfaces between the devices & transmission medium.
• Representation of bits: The physical layer is concerned with transmission of signals from one device to another which involves converting data (1_s & 0_s) into signals and vice versa. It is not concerned with the meaning or interpretation of bits.
• Data rate: The physical layer defines the data

transmission rate i.e. number of bits sent per second. It is the responsibility of the physical layer to maintain the defined data rate.

Data Communication and Computer Networking module | PDF page 16 | lines 43-47

Application Layer
• The application layer enables the user to communicate its data to the receiver by providing certain services.
• The main Responsibility of Application layer is to provide the user access to network resources.

Data Communication and Computer Networking module | PDF page 16 | lines 18-32

Session Layer
• The session layer establishes a session between the communicating devices called dialog and synchronizes their interaction. It is the responsibility of the session layer to establish and synchronize the dialogs. It is also called the network dialog controller.
• The session layer at the sending side accepts data from the presentation layer adds checkpoints to it called sync bits and passes the data to the transport layer. At the receiving end the session layer receives data from the transport layer removes the checkpoints inserted previously and passes the data to the presentation layer. So, the main responsibility of session layer is dialog control and synchronization.

Question sources

Computer Science MCQ practice collection · Question 499

Question 196 | AM0500

Which protocol is used for translating domain names into IP addresses?

A. DNS

B. FTP

C. HTTP

D. SMTP

Hint

Identify the requested service or delivery guarantee, then distinguish application roles, transport behavior and address configuration.

Answer A: DNS

DNS is the named external Domain Name Service, contrasted with host-address entries used without external naming. Evidence: PDF 18, 65.

Why each choice is right or wrong

A - Correct: DNS matches domain-to-address lookup (PDF 18, 65.)

B - Incorrect: FTP is file transfer (PDF 18, 65.)

C - Incorrect: HTTP is not the domain naming service (PDF 18, 65.)

D - Incorrect: SMTP is mail transfer (PDF 18, 65.)

Primary note proof

Study-note section NET20

> DNS resolves names to records, including IPv4 A and IPv6 AAAA addresses; it can use UDP or TCP port 53. DHCP dynamically leases IPv4 settings, commonly address, mask, gateway and DNS server. Its basic exchange is discover, offer, request, acknowledge. IP itself does not assign addresses.

Study-note section NET21

> HTTP defines web request/response semantics; it is stateless, and a message body may be absent. HTTPS adds TLS protection. FTP transfers files using control and separate data connections; it is not the same protocol as SFTP. SMTP submits and relays mail; POP3 retrieves messages and IMAP accesses/synchronizes server mailboxes. Saying SMTP handles both sending and end-user mailbox retrieval is inaccurate.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 18 | lines 27-32

> Application Layer
> The Application Layer is a combination of Session,
> Presentation & Application Layers of OSI models and defines
> high level protocols like File Transfer (FTP), Electronic Mail
> (SMTP), Virtual Terminal (TELNET), Domain Name Service
> (DNS), etc.

Data Communication and Computer Networking module | PDF page 65 | lines 31-38

> /etc/hosts
> The /etc/hosts file always contains the localhost IP
> address, 127.0.0.1, which is
> usedfor interprocess communication.
> Never remove this line! Sometimes contains
> addresses of additional hosts, whichcan be contacted
> without using an external naming service such as
> DNS (the Domain Name Server).

Question sources

Computer Science MCQ practice collection · Question 500

Question 197 | AM0501

Which layer of the OSI reference model is responsible for establishing and terminating sessions between applications?

A. Presentation layer

B. Session layer

C. Transport layer

D. Application layer

Hint

Match the requested scope or data unit to the layer duties in the note; distinguish hop delivery from end-to-end process delivery.

Answer B: Session layer

The session layer establishes communication dialogs and controls/synchronizes their interaction, matching the explicitly stated sessions between applications. Evidence: PDF 16, 16, 16, 16.

Why each choice is right or wrong

A - Incorrect: Presentation performs representation translation (PDF 16, 16, 16, 16.)

B - Correct: Session establishes and synchronizes dialogs (PDF 16, 16, 16, 16.)

C - Incorrect: Transport connection setup is a different scope from the stated application sessions (PDF 16, 16, 16, 16.)

D - Incorrect: Application provides user access to network services (PDF 16, 16, 16, 16.)

Primary note proof

Study-note section NET19

OSI session roles establish/manage dialogs and can coordinate checkpoints so transfer resumes after interruption. Presentation roles translate encodings and handle compression/encryption. Compression reduces representation size; encryption hides content and need not shrink it. Application protocols provide services directly to applications. Practical implementations distribute these functions differently; TLS is not proof of a separate physical presentation-layer device.

Study-note section NET18

TCP establishes state with SYN, SYN+ACK, then ACK. SYN consumes one sequence position even with no application bytes. An acknowledgment states the next expected sequence number. For client ISN=395 and server ISN=260: client sends SYN seq395; server sends SYN+ACK seq260 ack396; client sends ACK seq396 ack261. Later byte counts advance sequence numbers. FIN also consumes one sequence position.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 16 | lines 18-32

Session Layer
• The session layer establishes a session between the communicating devices called dialog and synchronizes their interaction. It is the responsibility of the session layer to establish and synchronize the dialogs. It is also called the network dialog controller.
• The session layer at the sending side accepts data from the presentation layer adds checkpoints to it called sync bits and passes the data to the transport layer. At the receiving end the session layer receives data from the transport layer removes the checkpoints inserted previously and passes the data to the presentation layer. So, the main responsibility of session layer is dialog control and synchronization.

Data Communication and Computer Networking module | PDF page 16 | lines 33-42

Presentation Layer
• The communicating devices may be having different platforms. The presentation layer performs translation, encryption and compression of data.
• The presentation layer receives the data from the application layer adds header which contains information related to encryption and compression and sends it to the session layer.
• So, the main responsibility of the Presentation layer is translation, compression and encryption.

Data Communication and Computer Networking module | PDF page 16 | lines 2-17

• At the sending side, the transport layer receives data from the session layer, divides it into units called segments and sends it to the network layer.
• To ensure process to process delivery the transport layer makes use of port address to identify the data from the sending and receiving process.
• The data can be transported in a connection oriented or connectionless manner.
• The Transport layer is responsible for segmentation and reassembly of the message into segments which bear sequence numbers.
• The transport layer also carries out flow control and error control functions; but unlike data link layer these are end to end rather than node to node.

• The main responsibility of the transport layer is process to process delivery of the entire message

Data Communication and Computer Networking module | PDF page 16 | lines 43-47

Application Layer
• The application layer enables the user to communicate its data to the receiver by providing certain services.
• The main Responsibility of Application layer is to provide the user access to network resources.

Question sources

Computer Science MCQ practice collection · Question 501

Question 198 | AM0502

A file-transfer client uses one connection for protocol commands and a separate connection for file data. Which listed application protocol uses this control/data separation?

A. SMTP

B. HTTP

C. FTP

D. TCP

Hint

Identify the requested service or delivery guarantee, then distinguish application roles, transport behavior and address configuration.

Answer C: FTP

FTP separates its control conversation from the data connection used for transfers. That architectural feature distinguishes it from the broad ability to download files, which HTTP also provides. SMTP handles mail submission and relay. TCP is the transport service on which an application protocol can build connections; it does not itself define FTP commands or the application's separate control and data roles.

Why each choice is right or wrong

A - Incorrect: SMTP defines mail transfer, not the described FTP control/data arrangement.

B - Incorrect: HTTP can transfer files, but does not define the described separate FTP control and data connections.

C - Correct: FTP uses separate control and data connections.

D - Incorrect: TCP provides transport connections; the application protocol defines their command/data roles.

Primary note proof

Study-note section NET21

HTTP defines web request/response semantics; it is stateless, and a message body may be absent. HTTPS adds TLS protection. FTP transfers files using control and separate data connections; it is not the same protocol as SFTP. SMTP submits and relays mail; POP3 retrieves messages and IMAP accesses/synchronizes server mailboxes. Saying SMTP handles both sending and end-user mailbox retrieval is inaccurate.

Study-note section NET17

TCP offers a reliable ordered byte stream using sequence numbers, acknowledgments, retransmission and windows. Flow control protects the receiver; congestion control protects network capacity. UDP sends independent datagrams with ports and a checksum but no built-in setup, delivery guarantee, retransmission or ordering. Live interactive traffic may choose UDP when late data is less useful than lost data. Application protocols can add reliability over UDP.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 18 | lines 27-32

Application Layer
The Application Layer is a combination of Session,
Presentation & Application Layers of OSI models and defines
high level protocols like File Transfer (FTP), Electronic Mail
(SMTP), Virtual Terminal (TELNET), Domain Name Service
(DNS), etc.

Data Communication and Computer Networking module | PDF page 18 | lines 9-21

TCP - Transmission Control Protocol: TCP is a reliable
connection-oriented, reliable protocol. i.e. a connection is
established between the sender and receiver before the data can
be transmitted. It divides the data it receives from the upper
layer into segments and tags a sequence number to each
segment which is used at the receiving end for reordering of
data.
UDP - User Datagram Protocol: UDP is a simple protocol
used for process to process transmission. It is an unreliable,
connectionless protocol for applications that do not require flow
control or error control. It simply adds port address, checksum
and length information to the data it receives from the upper
layer.

Question sources

Computer Science MCQ practice collection · Question 502

Question 199 | AM0503

Which layer of the OSI reference model is responsible for providing services directly to the end-user applications?

A. Presentation layer

B. Session layer

C. Transport layer

D. Application layer

Hint

Match the requested scope or data unit to the layer duties in the note; distinguish hop delivery from end-to-end process delivery.

Answer D: Application layer

Application explicitly provides user access to network resources; the other layers perform representation, dialog and process-delivery work. Evidence: PDF 16, 16, 16, 16.

Why each choice is right or wrong

A - Incorrect: Presentation translates/encrypts/compresses (PDF 16, 16, 16, 16.)

B - Incorrect: Session establishes and synchronizes dialogs (PDF 16, 16, 16, 16.)

C - Incorrect: Transport segments and delivers between processes (PDF 16, 16, 16, 16.)

D - Correct: Application explicitly exposes network resources to users (PDF 16, 16, 16, 16.)

Primary note proof

Study-note section NET19

> OSI session roles establish/manage dialogs and can coordinate checkpoints so transfer resumes after interruption. Presentation roles translate encodings and handle compression/encryption. Compression reduces representation size; encryption hides content and need not shrink it. Application protocols provide services directly to applications. Practical implementations distribute these functions differently; TLS is not proof of a separate physical presentation-layer device.

Study-note section NET17

> TCP offers a reliable ordered byte stream using sequence numbers, acknowledgments, retransmission and windows. Flow control protects the receiver; congestion control protects network capacity. UDP sends independent datagrams with ports and a checksum but no built-in setup, delivery guarantee, retransmission or ordering. Live interactive traffic may choose UDP when late data is less useful than lost data. Application protocols can add reliability over UDP.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 16 | lines 43-47

Application Layer
• The application layer enables the user to communicate its data to the receiver by providing certain services.
• The main Responsibility of Application layer is to provide the user access to network resources.

Data Communication and Computer Networking module | PDF page 16 | lines 33-42

Presentation Layer
• The communicating devices may be having different platforms. The presentation layer performs translation, encryption and compression of data.
• The presentation layer receives the data from the application layer adds header which contains information related to encryption and compression and sends it to the session layer.
• So, the main responsibility of the Presentation layer is translation, compression and encryption.

Data Communication and Computer Networking module | PDF page 16 | lines 18-32

Session Layer
• The session layer establishes a session between the communicating devices called dialog and synchronizes their interaction. It is the responsibility of the session layer to establish and synchronize the dialogs. It is also called the network dialog controller.
• The session layer at the sending side accepts data from the presentation layer adds checkpoints to it called sync bits and passes the data to the transport layer. At the receiving end the session layer receives data from the transport layer removes the checkpoints inserted previously and passes the data to the presentation layer. So, the main responsibility of session layer is dialog control and synchronization.

Data Communication and Computer Networking module | PDF page 16 | lines 2-17

• At the sending side, the transport layer receives data from the session layer, divides it into units called segments and sends it to the network layer.
• To ensure process to process delivery the transport layer makes use of port address to identify the data from the sending and receiving process.
• The data can be transported in a connection oriented or connectionless manner.
• The Transport layer is responsible for segmentation and reassembly of the message into segments which bear sequence numbers.

• The transport layer also carries out flow control and error control functions; but unlike data link layer these are end to end rather than node to node.
• The main responsibility of the transport layer is process to process delivery of the entire message

Question sources

Computer Science MCQ practice collection · Question 503

Question 200 | AM0504

Which subnet mask represents a Class C network?

A. 255.0.0.0

B. 255.255.0.0

C. 255.255.255.0

D. 255.255.255.255

Hint

Convert the mask to a prefix, separate network and host bits, and apply the relevant subnet-count or usable-host rule.

Answer C: 255.255.255.0, the historical Class C default

In the classful convention requested, Class C has a /24 default. Twenty-four leading one bits give three full 255 octets followed by zero: 255.255.255.0. This is a historical default rather than a restriction that every modern address in that range must use /24; CIDR can specify another prefix.

Why each choice is right or wrong

A - Incorrect: 255.0.0.0 is /8, the historical Class A default rather than Class C.

B - Incorrect: 255.255.0.0 is /16, the historical Class B default.

C - Correct: 255.255.255.0 is /24, matching the historical Class C default prefix.

D - Incorrect: 255.255.255.255 is /32, identifying one address rather than the Class C default network.

Primary note proof

Study-note section NET22

Historical classes use leading patterns: A 0 with /8, B 10 with /16, C 110 with /24; D 1110 is multicast and E 1111 reserved. Ordinary class-A first octets are 1-126 because 0 and 127 have special uses. B spans 128-191 and C 192-223. Default usable counts are 2^24-2, 2^16-2 and 254. Modern CIDR requires the actual prefix and overrides class defaults.

Study-note section NET24

A /p IPv4 prefix has p leading one bits followed by 32-p zeros. Partial octet masks are 128,192,224,240,248,252,254. /19 is 255.255.224.0; /20 is 255.255.240.0; /21 is 255.255.248.0, correcting the study guide's 255.248.0.0 mistake.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 19 | lines 23-36

Classful addressing : In classful addressing, the addressspace is divided into five classes: A, B, C, D, and E.
• Netid and Hostid In classful addressing, an IP addressin class A, B, or C is divided into netid and hostid.
Subnetting: It allows a network to be split into several parts for internal use but still act like a single network to the outsideworld.
• To implement subnetting, the router needs a subnet mask that indicates the split between network + subnet number and host. Ex. 255.255.252.0/22. A‖/22‖ to indicate that the subnet mask is 22 bits long.

Data Communication and Computer Networking module | PDF page 19 | lines 37-44

CIDR: A class B address is far too large for most organizationsand a class C network, with 256 addresses is too small. This leads to granting Class B address to organizations who do not require all. This is resulting in depletion of Address space. A solution is CIDR (Classless InterDomain Routing) The basic idea behind CIDR, is to allocate the remaining IP addresses in variable-sized blocks, without regard to the classes.

Question sources

Computer Science MCQ practice collection · Question 504

Question 201 | AM0505

What is the maximum number of hosts in a subnet with a subnet mask of 255.255.255.224?

A. 8

B. 16

C. 30

D. 62

Hint

Convert the mask to a prefix, separate network and host bits, and apply the relevant subnet-count or usable-host rule.

Answer C: 30 usable hosts

The mask 255.255.255.224 has 27 one bits and five host bits. Five bits yield 32 total addresses; reserving the subnet identifier and directed broadcast leaves 30 assignable ordinary hosts. This is an ordinary broadcast-subnet calculation, so the special /31 point-to-point exception is not relevant.

Why each choice is right or wrong

A - Incorrect: Eight does not equal the usable count from five host bits and two reserved addresses.

B - Incorrect: Sixteen is not the /27 usable-host count; this block has 32 total addresses.

C - Correct: A /27 has 32 total addresses and 30 ordinary assignable host addresses.

D - Incorrect: Sixty-two usable hosts requires six host bits, corresponding to /26 rather than /27.

Primary note proof

Study-note section NET25

> For ordinary broadcast LANs let h=32-p. Total addresses=2^h; usable hosts=2^h-2, reserving network and directed broadcast. Find the changing octet's increment as 256-mask octet, round the address down to a multiple, and extend through the next boundary minus one.

Study-note section NET24

> A /p IPv4 prefix has p leading one bits followed by 32-p zeros. Partial octet masks are 128,192,224,240,248,252,254. /19 is 255.255.224.0; /20 is 255.255.240.0; /21 is 255.255.248.0, correcting the study guide's 255.248.0.0 mistake.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 19 | lines 2-22

> Address Space: An address space is the total
> number ofaddresses used by the protocol.
> • If a protocol uses N bits to define an address,
> the address space is 2N
> because each bit can
> have twodifferent values (0 or 1) and N bits
> can have 2N values.
> • IPv4 uses 32-bit addresses, which means that
> the address space is 232 or 4,294,967,296
> (more than 4billion).
> Notations: There are two notations to show an IPv4 address:
> • Binary notation: The IPv4 address is displayed

as 32bits. ex. 11000001 10000011 00011011 11111111
• Dotted decimal notation: To make the IPv4 address easier to read, Internet addresses are usually written in decimal form with a decimal point (dot) separatingthe bytes. Each byte (octet) is 8 bits hence each number in dotted-decimal notation is a value rangingfrom 0 to 255. Ex. 129.11.11.239

Data Communication and Computer Networking module | PDF page 19 | lines 23-36

Classful addressing : In classful addressing, the addressspace is divided into five classes: A, B, C, D, and E.
• Netid and Hostid In classful addressing, an IP addressin class A, B, or C is divided into netid and hostid.
Subnetting: It allows a network to be split into several parts for internal use but still act like a single network to the outsideworld.
• To implement subnetting, the router needs a subnet mask that indicates the split between network + subnet number and host. Ex. 255.255.252.0/22. A‖/22‖ to indicate that the subnet mask is 22 bits long.

Question sources

Computer Science MCQ practice collection · Question 505

Question 202 | AM0506

Which IP address belongs to the loopback network?

A. 127.0.0.1

B. 192.168.0.1

C. 10.0.0.1

D. 172.16.0.1

Hint

Separate address width, syntax, reserved scope and the supplied prefix or historical classful convention.

Answer A: 127.0.0.1

The module explicitly identifies 127.0.0.1 as localhost for interprocess communication. This supports the loopback instance, without needing an unprovided full 127/8 range rule. Evidence: PDF 65, 19.

Why each choice is right or wrong

A - Correct: 127.0.0.1 is explicitly localhost (PDF 65, 19.)

B - Incorrect: 192.168.0.1 is not the cited localhost address (PDF 65, 19.)

C - Incorrect: 10.0.0.1 is not the cited localhost address (PDF 65, 19.)

D - Incorrect: 172.16.0.1 is not the cited localhost address (PDF 65, 19.)

Primary note proof

Study-note section NET23

> RFC1918 private blocks are 10.0.0.0/8, 172.16.0.0/12 (through 172.31.255.255), and 192.168.0.0/16. They can be reused internally but are not globally routed as public destinations. A LAN may also use legitimately assigned public addresses; private is common, not mandatory. 127.0.0.0/8 is IPv4 loopback, commonly 127.0.0.1, for local protocol access without an external link. 255.255.255.255 is limited broadcast; 0.0.0.0 can identify an unconfigured source. Link-local/APIPA uses 169.254.0.0/16, with edge /24 blocks excluded from normal automatic selection.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 65 | lines 31-38

> /etc/hosts
> The /etc/hosts file always contains the localhost IP
> address, 127.0.0.1, which is
> usedfor interprocess communication.
> Never remove this line! Sometimes contains
> addresses of additional hosts, whichcan be contacted
> without using an external naming service such as
> DNS (the Domain Name Server).

Data Communication and Computer Networking module | PDF page 19 | lines 45-49

> NAT (Network Address Translation): The scarcity of
> network addresses in IPv4 led to the development of IPv6.
> Due to this, we need to use private IP address inside the
> organization and translate it to public IP address using
> NAT.

Question sources

Computer Science MCQ practice collection · Question 506

Question 203 | AM0507

How many subnets can be created from a Class B network with a subnet mask of 255.255.240.0?

A. 8

B. 16

C. 32

D. 64

Hint

Convert the mask to a prefix, separate network and host bits, and apply the relevant subnet-count or usable-host rule.

Answer B: 16 subnets

The question explicitly supplies a Class B parent, so use its historical /16. The given mask 255.255.240.0 is /20. Borrowing 20−16=4 bits yields 2^4=16 equal subnets under modern practice. The note says not to subtract two subnets; host capacity is a different calculation.

Why each choice is right or wrong

A - Incorrect: Eight subnets would borrow three bits and produce /19 from a /16 parent.

B - Correct: The /20 mask borrows four bits from /16, yielding sixteen equal subnets.

C - Incorrect: Thirty-two subnets would borrow five bits and require /21 from the Class B parent.

D - Incorrect: Sixty-four subnets would borrow six bits and require /22 rather than /20.

Primary note proof

Study-note section NET26

> To split parent /a into equal /p blocks, borrow b=p-a bits and obtain 2^b subnets. Do not subtract two subnets under modern practice. For a Class B /16 parent split to /19, b=3 gives eight subnets, each with 8192 addresses and 8190 conventional hosts. A /19 alone does not state its parent.

Study-note section NET22

> Historical classes use leading patterns: A 0 with /8, B 10 with /16, C 110 with /24; D 1110 is multicast and E 1111 reserved. Ordinary class-A first octets are 1-126 because 0 and 127 have special uses. B spans 128-191 and C 192-223. Default usable counts are 2^24-2, 2^16-2 and 254. Modern CIDR requires the actual prefix and overrides class defaults.

Study-note section NET24

> A /p IPv4 prefix has p leading one bits followed by 32-p zeros. Partial octet masks are 128,192,224,240,248,252,254. /19 is 255.255.224.0; /20 is 255.255.240.0; /21 is 255.255.248.0, correcting the study guide’s 255.248.0.0 mistake.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 19 | lines 2-22

Address Space: An address space is the total number ofaddresses used by the protocol.
• If a protocol uses N bits to define an address, the address space is 2N because each bit can have twodifferent values (0 or 1) and N bits can have 2N values.
• IPv4 uses 32-bit addresses, which means that the address space is 232 or 4,294,967,296 (more than 4billion).
Notations: There are two notations to show an IPv4 address:
• Binary notation: The IPv4 address is displayed as 32bits. ex. 11000001 10000011 00011011 11111111
• Dotted decimal notation: To make the IPv4 address easier to read, Internet addresses are usually written in decimal form with a decimal point (dot) separatingthe bytes. Each byte (octet) is 8 bits hence each number in dotted-decimal notation is a value rangingfrom 0 to 255. Ex. 129.11.11.239

Data Communication and Computer Networking module | PDF page 19 | lines 23-36

Classful addressing : In classful addressing, the addressspace is divided into five classes: A, B, C, D, and E.
• Netid and Hostid In classful addressing, an IP addressin class A, B, or C is divided into netid and hostid.
Subnetting: It allows a network to be split into several parts for internal use but still act like a single network to the outsideworld.
• To implement subnetting, the router needs a subnet mask that indicates the split between network + subnet number and host. Ex. 255.255.252.0/22. A‖/22‖ to indicate that the subnet mask is 22 bits long.

Question sources

Computer Science MCQ practice collection · Question 507

Question 204 | AM0508

What is the default subnet mask for a Class A network?

A. 255.0.0.0

B. 255.255.0.0

C. 255.255.255.0

D. 255.255.255.255

Hint

Convert the mask to a prefix, separate network and host bits, and apply the relevant subnet-count or usable-host rule.

Answer A: 255.0.0.0

The historical Class A default is /8. Eight leading mask ones fill only the first octet, giving 255.0.0.0. The other choices correspond to /16, /24 and /32; they can be explicit CIDR prefixes, but they are not the historical default asked for.

Why each choice is right or wrong

A - Correct: 255.0.0.0 contains eight leading ones and is the historical Class A default.

B - Incorrect: 255.255.0.0 is /16, the historical default for Class B.

C - Incorrect: 255.255.255.0 is /24, the historical default for Class C.

D - Incorrect: 255.255.255.255 is /32 and describes one address, not the Class A default.

Primary note proof

Study-note section NET22

> Historical classes use leading patterns: A 0 with /8, B 10 with /16, C 110 with /24; D 1110 is multicast and E 1111 reserved. Ordinary class-A first octets are 1-126 because 0 and 127 have special uses. B spans 128-191 and C 192-223. Default usable counts are 2^24-2, 2^16-2 and 254. Modern CIDR requires the actual prefix and overrides class defaults.

Study-note section NET24

> A /p IPv4 prefix has p leading one bits followed by 32-p zeros. Partial octet masks are 128,192,224,240,248,252,254. /19 is 255.255.224.0; /20 is 255.255.240.0; /21 is 255.255.248.0, correcting the study guide’s 255.248.0.0 mistake.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 19 | lines 23-36

> Classful addressing : In classful addressing, the
> addressspace is divided into five classes: A, B, C,
> D, and E.
> • Netid and Hostid In classful addressing, an IP

addressin class A, B, or C is divided into netid
and hostid.
Subnetting: It allows a network to be split into several
parts for internal use but still act like a single network to
the outsideworld.
• To implement subnetting, the router needs a
subnet mask that indicates the split between
network + subnet number and host. Ex.
255.255.252.0/22. A‖/22‖ to indicate that the
subnet mask is 22 bits long.

Data Communication and Computer Networking module | PDF page 19 | lines 2-22

Address Space: An address space is the total
number ofaddresses used by the protocol.
• If a protocol uses N bits to define an address,
the address space is 2N
because each bit can
have twodifferent values (0 or 1) and N bits
can have 2N values.
• IPv4 uses 32-bit addresses, which means that
the address space is 232 or 4,294,967,296
(more than 4billion).
Notations: There are two notations to show an IPv4 address:
• Binary notation: The IPv4 address is displayed
as 32bits. ex. 11000001 10000011 00011011
11111111
• Dotted decimal notation: To make the IPv4
address easier to read, Internet addresses are
usually written in decimal form with a decimal
point (dot) separatingthe bytes. Each byte (octet)
is 8 bits hence each number in dotted-decimal
notation is a value rangingfrom 0 to 255. Ex.
129.11.11.239

Question sources

Computer Science MCQ practice collection · Question 508

Question 205 | AM0509

For a conventional IPv4 link needing two usable endpoints and reserving network/broadcast addresses, which offered mask allocates the smallest sufficient block?

A. 255.255.255.0

B. 255.255.255.128

C. 255.255.255.192

D. 255.255.255.252

Hint

Separate address width, syntax, reserved scope and the supplied prefix or historical classful convention.

Answer D: 255.255.255.252

The offered masks correspond to /24, /25, /26 and /30 blocks. A conventional /30 contains four addresses, leaving two usable endpoints after reserving network and broadcast addresses. The other choices allocate more addresses than this link needs. Supported /31 point-to-point links are a separate exception, so the question limits the comparison to the conventional model and the masks actually offered.

Why each choice is right or wrong

A - Incorrect: /24 is sufficient but allocates 256 addresses, more than the smallest offered sufficient block.

B - Incorrect: /25 allocates 128 addresses and is not the smallest sufficient offered block.

C - Incorrect: /26 allocates 64 addresses and is not the smallest sufficient offered block.

D - Correct: /30 allocates four addresses and two conventional usable endpoints, the smallest sufficient offered block.

Primary note proof

Study-note section NET28

> A conventional /30 has four addresses and two usable endpoints; check the link and addressing assumptions when selecting a WAN prefix. RFC3021 permits /31 on supported point-to-point links: both addresses are endpoints, so the subtract-two rule does not apply. /32 identifies one address/host route. Do not claim /30 is universally the smallest valid link prefix.

Study-note section NET24

> A /p IPv4 prefix has p leading one bits followed by 32-p zeros. Partial octet masks are 128,192,224,240,248,252,254. /19 is 255.255.224.0; /20 is 255.255.240.0; /21 is 255.255.248.0, correcting the study guide’s 255.248.0.0 mistake.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 19 | lines 2-22

Address Space: An address space is the total
number ofaddresses used by the protocol.
• If a protocol uses N bits to define an address,
the address space is 2N
because each bit can
have twodifferent values (0 or 1) and N bits
can have 2N values.
• IPv4 uses 32-bit addresses, which means that
the address space is 232 or 4,294,967,296
(more than 4billion).
Notations: There are two notations to show an IPv4 address:
• Binary notation: The IPv4 address is displayed
as 32bits. ex. 11000001 10000011 00011011
11111111
• Dotted decimal notation: To make the IPv4
address easier to read, Internet addresses are
usually written in decimal form with a decimal
point (dot) separatingthe bytes. Each byte (octet)
is 8 bits hence each number in dotted-decimal
notation is a value rangingfrom 0 to 255. Ex.
129.11.11.239

Data Communication and Computer Networking module | PDF page 19 | lines 23-36

Classful addressing : In classful addressing, the
addressspace is divided into five classes: A, B, C,
D, and E.
• Netid and Hostid In classful addressing, an IP
addressin class A, B, or C is divided into netid
and hostid.
Subnetting: It allows a network to be split into several
parts for internal use but still act like a single network to
the outsideworld.
• To implement subnetting, the router needs a
subnet mask that indicates the split between
network + subnet number and host. Ex.
255.255.252.0/22. A‖/22‖ to indicate that the
subnet mask is 22 bits long.

Data Communication and Computer Networking module | PDF page 11 | lines 34-51

NETWORK TOPOLOGY
A network topology is a description of the layout of the region
or area covered by that network.
There are two types of connections. They are: point-to-point
and multi-point.
Point-to-point connections provide a direct link between two
devices.
Multi-point connections provide a link between three or more

devices on a network.
There are seven basic topologies in the study of network topology:
• Point-to-point topology,
• Bus (point-to-multipoint) topology,
• Ring topology,
• Star topology,
• Hybrid topology,
• Mesh topology and,
• Tree topology.

Question sources

Computer Science MCQ practice collection · Question 509

Question 206 | AM0510

How many bits are in the host portion of an IPv4 address with a subnet mask of 255.255.255.192?

A. 6

B. 8

C. 10

D. 14

Hint

Convert the mask to a prefix, separate network and host bits, and apply the relevant subnet-count or usable-host rule.

Answer A: 6

192=11000000 leaves six zero mask bits; the full mask is /26. Hence 32-26=6 host bits. Evidence: PDF 18, 19, 19.

Why each choice is right or wrong

A - Correct: Six is the calculated count (PDF 18, 19, 19.)

B - Incorrect: Eight would correspond to /24 (PDF 18, 19, 19.)

C - Incorrect: Ten would correspond to /22 (PDF 18, 19, 19.)

D - Incorrect: Fourteen would correspond to /18 (PDF 18, 19, 19.)

Primary note proof

Study-note section NET24

A /p IPv4 prefix has p leading one bits followed by 32-p zeros. Partial octet masks are 128,192,224,240,248,252,254. /19 is 255.255.224.0; /20 is 255.255.240.0; /21 is 255.255.248.0, correcting the study guide's 255.248.0.0 mistake.

Study-note section NET25

For ordinary broadcast LANs let h=32-p. Total addresses=2^h; usable hosts=2^h-2, reserving network and directed broadcast. Find the changing octet's increment as 256-mask octet, round the address down to a multiple, and extend through the next boundary minus one.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 18 | lines 45-54

IP addresses: IP address uniquely identifies a device on the
Internet. Every host and router on the Internet has an IP address,
which encodes its network number and host number.
• The combination is unique: in principle, no two
machines on the Internet have the same IP address.
• An IPv4 address is 32 bits long
• They are used in the Source address and Destination
address fields of IP packets.
• An IP address does not refer to a host but it refers to a
network interface.

Data Communication and Computer Networking module | PDF page 19 | lines 2-22

Address Space: An address space is the total
number ofaddresses used by the protocol.
• If a protocol uses N bits to define an address,
the address space is 2N
because each bit can
have twodifferent values (0 or 1) and N bits
can have 2N values.
• IPv4 uses 32-bit addresses, which means that
the address space is 232 or 4,294,967,296
(more than 4billion).
Notations: There are two notations to show an IPv4 address:
• Binary notation: The IPv4 address is displayed
as 32bits. ex. 11000001 10000011 00011011
11111111
• Dotted decimal notation: To make the IPv4
address easier to read, Internet addresses are
usually written in decimal form with a decimal
point (dot) separatingthe bytes. Each byte (octet)
is 8 bits hence each number in dotted-decimal
notation is a value rangingfrom 0 to 255. Ex.
129.11.11.239

Data Communication and Computer Networking module | PDF page 19 | lines 23-36

Classful addressing : In classful addressing, the addressspace is divided into five classes: A, B, C, D, and E.
• Netid and Hostid In classful addressing, an IP addressin class A, B, or C is divided into netid and hostid.
Subnetting: It allows a network to be split into several parts for internal use but still act like a single network to the outsideworld.
• To implement subnetting, the router needs a subnet mask that indicates the split between network + subnet number and host. Ex. 255.255.252.0/22. A‖/22‖ to indicate that the subnet mask is 22 bits long.

Question sources

Computer Science MCQ practice collection · Question 510

Question 207 | AM0511

What is the network address for the IP address 192.168.10.25/28?

A. 192.168.10.0

B. 192.168.10.16

C. 192.168.10.24

D. 192.168.10.25

Hint

Convert the mask to a prefix, separate network and host bits, and apply the relevant subnet-count or usable-host rule.

Answer B: 192.168.10.16

/28 mask last octet is 240. 25=00011001 AND 240=11110000 gives 16=00010000. Therefore network address is 192.168.10.16. Evidence: PDF 18, 19, 19.

Why each choice is right or wrong

A - Incorrect: 0 is the preceding /28 block (PDF 18, 19, 19.)

B - Correct: 16 is the correct masked boundary (PDF 18, 19, 19.)

C - Incorrect: 24 retains host bits and is not a 16-step boundary (PDF 18, 19, 19.)

D - Incorrect: 25 is the given host address, not the masked network (PDF 18, 19, 19.)

Primary note proof

Study-note section NET24

Compute network=address AND mask. Host bits zero identify the block start; host bits one give broadcast. With 172.16.28.252/20, the third octet is grouped in blocks of 16, so the network is 172.16.16.0 and broadcast 172.16.31.255. A written host/prefix such as 172.105.180.0/21 need not be an aligned block label: masking yields 172.105.176.0/21.

Study-note section NET25

192.168.2.64/26 spans .64-.127; usable .65-.126 gives 62 hosts. 192.168.10.25/28 spans .16-.31, so its network is .16. 172.17.128.0/21 spans 172.17.128.0-172.17.135.255; .128.255 and .135.0 are valid interior hosts, but .135.255 is broadcast. /27 gives 32 total and 30 usable, not 32 usable.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 18 | lines 45-54

IP addresses: IP address uniquely identifies a device on the
Internet. Every host and router on the Internet has an IP address,
which encodes its network number and host number.
• The combination is unique: in principle, no two
machines on the Internet have the same IP address.
• An IPv4 address is 32 bits long
• They are used in the Source address and Destination
address fields of IP packets.
• An IP address does not refer to a host but it refers to a
network interface.

Data Communication and Computer Networking module | PDF page 19 | lines 2-22

Address Space: An address space is the total
number ofaddresses used by the protocol.
• If a protocol uses N bits to define an address,
the address space is 2N
because each bit can
have twodifferent values (0 or 1) and N bits
can have 2N values.
• IPv4 uses 32-bit addresses, which means that
the address space is 232 or 4,294,967,296
(more than 4billion).
Notations: There are two notations to show an IPv4 address:
• Binary notation: The IPv4 address is displayed
as 32bits. ex. 11000001 10000011 00011011
11111111
• Dotted decimal notation: To make the IPv4
address easier to read, Internet addresses are
usually written in decimal form with a decimal
point (dot) separatingthe bytes. Each byte (octet)

is 8 bits hence each number in dotted-decimal notation is a value rangingfrom 0 to 255. Ex. 129.11.11.239

Data Communication and Computer Networking module | PDF page 19 | lines 23-36

Classful addressing : In classful addressing, the addressspace is divided into five classes: A, B, C, D, and E.
• Netid and Hostid In classful addressing, an IP addressin class A, B, or C is divided into netid and hostid.
Subnetting: It allows a network to be split into several parts for internal use but still act like a single network to the outsideworld.
• To implement subnetting, the router needs a subnet mask that indicates the split between network + subnet number and host. Ex. 255.255.252.0/22. A‖/22‖ to indicate that the subnet mask is 22 bits long.

Question sources

Computer Science MCQ practice collection · Question 511

Question 208 | AM0512

How many usable host addresses are available in a subnet with a subnet mask of 255.255.255.224?

A. 6

B. 14

C. 30

D. 62

Hint

Convert the mask to a prefix, separate network and host bits, and apply the relevant subnet-count or usable-host rule.

Answer C: 30 usable host addresses

224 in the final mask octet is 11100000. That yields /27 and h=5. Computing 2^5−2 gives 30 ordinary usable host addresses after network and directed-broadcast reservations. The distractors correspond to different host-bit counts; none changes the explicit mask in this question.

Why each choice is right or wrong

A - Incorrect: Six usable hosts would use three host bits, normally /29 rather than /27.

B - Incorrect: Fourteen usable hosts would use four host bits, normally /28.

C - Correct: Five host bits give 32 addresses minus two reservations, yielding 30 usable hosts.

D - Incorrect: Sixty-two usable hosts would use six host bits and a /26 mask.

Primary note proof

Study-note section NET25

> For ordinary broadcast LANs let h=32-p. Total addresses=2^h; usable hosts=2^h-2, reserving network and directed broadcast. Find the changing octet's increment as 256-mask octet, round the address down to a multiple, and extend through the next boundary minus one.

Study-note section NET24

> A /p IPv4 prefix has p leading one bits followed by 32-p zeros. Partial octet masks are 128,192,224,240,248,252,254. /19 is 255.255.224.0; /20 is 255.255.240.0; /21 is 255.255.248.0, correcting the study guide's 255.248.0.0 mistake.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 19 | lines 2-22

> Address Space: An address space is the total
> number ofaddresses used by the protocol.
> • If a protocol uses N bits to define an address,
> the address space is 2N
> because each bit can
> have twodifferent values (0 or 1) and N bits
> can have 2N values.
> • IPv4 uses 32-bit addresses, which means that
> the address space is 232 or 4,294,967,296
> (more than 4billion).
> Notations: There are two notations to show an IPv4 address:
> • Binary notation: The IPv4 address is displayed
> as 32bits. ex. 11000001 10000011 00011011
> 11111111
> • Dotted decimal notation: To make the IPv4
> address easier to read, Internet addresses are
> usually written in decimal form with a decimal
> point (dot) separatingthe bytes. Each byte (octet)
> is 8 bits hence each number in dotted-decimal
> notation is a value rangingfrom 0 to 255. Ex.
> 129.11.11.239

Data Communication and Computer Networking module | PDF page 19 | lines 23-36

Classful addressing : In classful addressing, the addressspace is divided into five classes: A, B, C, D, and E.
• Netid and Hostid In classful addressing, an IP addressin class A, B, or C is divided into netid and hostid.
Subnetting: It allows a network to be split into several parts for internal use but still act like a single network to the outsideworld.
• To implement subnetting, the router needs a subnet mask that indicates the split between network + subnet number and host. Ex. 255.255.252.0/22. A‖/22‖ to indicate that the subnet mask is 22 bits long.

Question sources

Computer Science MCQ practice collection · Question 512

Question 209 | AM0513

Which address category is defined for internal reuse by RFC1918 rather than global public routing?

A. Public IP address

B. Private IP address

C. Reserved IP address

D. Dynamic IP address

Hint

Use the cited note definitions to identify the requested function or scope, then check each alternative against that same rule.

Answer B: Private IP address

RFC1918 defines private blocks that organizations can reuse internally and that are not globally routed as public destinations. Public addresses can also be used on a LAN when legitimately assigned, so local communication alone would not distinguish the categories. Dynamic describes an assignment method such as a DHCP lease, not an address scope. The revised scope identifies the category by its defined allocation purpose.

Why each choice is right or wrong

A - Incorrect: Public addresses are globally allocated unicast space rather than RFC1918 internal-reuse space.

B - Correct: Private addresses are the RFC1918 blocks defined for internal reuse.

C - Incorrect: Reserved addresses have specific purposes and are not a generic ordinary-LAN host address category.

D - Incorrect: Dynamic describes how an address is assigned, not whether it belongs to RFC1918 space.

Primary note proof

Study-note section NET23

RFC1918 private blocks are 10.0.0.0/8, 172.16.0.0/12 (through 172.31.255.255), and 192.168.0.0/16. They can be reused internally but are not globally routed as public destinations. A LAN may also use legitimately assigned public addresses; private is common, not mandatory. 127.0.0.0/8 is IPv4 loopback, commonly 127.0.0.1, for local protocol access without an external link. 255.255.255.255 is limited broadcast; 0.0.0.0 can identify an unconfigured source. Link-local/APIPA uses 169.254.0.0/16, with edge /24 blocks excluded from normal automatic selection.

Study-note section NET20

DNS resolves names to records, including IPv4 A and IPv6 AAAA addresses; it can use UDP or TCP port 53. DHCP dynamically leases IPv4 settings, commonly address, mask, gateway and DNS server. Its basic exchange is discover, offer, request, acknowledge. IP itself does not assign addresses.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 19 | lines 45-49

NAT (Network Address Translation): The scarcity of
network addresses in IPv4 led to the development of IPv6.
Due to this, we need to use private IP address inside the
organization and translate it to public IP address using
NAT.

Data Communication and Computer Networking module | PDF page 48 | lines 29-40

Network Address Translation (NAT)
NAT translates the IP addresses of computers in a local
network to a single IP address. This address is often used
by the router that connects the computers to the Internet.
The router can be connected to a DSL modem, cable
modem, T1 line, or even a dial-up modem. When other
computers on the Internet attempt to access computers
within the local network, they only see the IP address of
the router. This adds an extra level of security, since the
router can be configured as a firewall, only allowing
authorized systems to access the computers within the
network.

Question sources

Computer Science MCQ practice collection · Question 513

Question 210 | AM0514

Which of the following is not a valid IP address?

A. 192.168.0.1

B. 10.0.0.256

C. 172.16.0.0

D. 255.255.255.0

Hint

Separate address width, syntax, reserved scope and the supplied prefix or historical classful convention.

Answer B: 10.0.0.256

Each IPv4 decimal octet must be 0-255. 10.0.0.256 violates that constraint; the other strings are syntactically valid IPv4 values regardless of host-assignability restrictions. Evidence: PDF 19.

Why each choice is right or wrong

A - Incorrect: All four octets satisfy the syntax rule (PDF 19.)

B - Correct: 256 exceeds the eight-bit maximum (PDF 19.)

C - Incorrect: All octets are syntactically valid; a network-address role is a separate issue (PDF 19.)

D - Incorrect: All octets are syntactically valid; use as a mask does not make the bit string invalid (PDF 19.)

Primary note proof

Study-note section NET22

> Write IPv4 as four decimal octets 0-255, or as 32 binary bits. Use weights 128,64,32,16,8,4,2,1 within each octet. Thus 11000001 10000011 00011011 11111111 is 193.131.27.255. A value such as 257 is impossible. Syntactic validity differs from assignability: an address ending .0 or .255 can be a host under some prefixes.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 19 | lines 2-22

> Address Space: An address space is the total
> number ofaddresses used by the protocol.
> • If a protocol uses N bits to define an address,
> the address space is 2N
> because each bit can
> have twodifferent values (0 or 1) and N bits
> can have 2N values.
> • IPv4 uses 32-bit addresses, which means that

the address space is 232 or 4,294,967,296
(more than 4billion).
Notations: There are two notations to show an IPv4 address:
• Binary notation: The IPv4 address is displayed
as 32bits. ex. 11000001 10000011 00011011
11111111
• Dotted decimal notation: To make the IPv4
address easier to read, Internet addresses are
usually written in decimal form with a decimal
point (dot) separatingthe bytes. Each byte (octet)
is 8 bits hence each number in dotted-decimal
notation is a value rangingfrom 0 to 255. Ex.
129.11.11.239

Question sources

Computer Science MCQ practice collection · Question 514

Question 211 | AM0515

What is the default subnet mask for a Class B IP address?

A. 255.0.0.0

B. 255.255.0.0

C. 255.255.255.0

D. 255.255.255.255

Hint

Convert the mask to a prefix, separate network and host bits, and apply the relevant subnet-count or usable-host rule.

Answer B: 255.255.0.0

NET22 gives historical Class B a /16 default. The first sixteen mask bits are ones, producing 255.255.0.0. This answers the requested default-mask question; it does not imply that a modern Class B-range address cannot have a different explicit CIDR prefix.

Why each choice is right or wrong

A - Incorrect: 255.0.0.0 is /8, the historical default for Class A.

B - Correct: 255.255.0.0 has sixteen leading ones and is the historical Class B default.

C - Incorrect: 255.255.255.0 is /24, the historical default for Class C.

D - Incorrect: 255.255.255.255 is /32, a single-address prefix rather than a Class B default.

Primary note proof

Study-note section NET22

Historical classes use leading patterns: A 0 with /8, B 10 with /16, C 110 with /24; D 1110 is multicast and E 1111 reserved. Ordinary class-A first octets are 1-126 because 0 and 127 have special uses. B spans 128-191 and C 192-223. Default usable counts are 2^24-2, 2^16-2 and 254. Modern CIDR requires the actual prefix and overrides class defaults.

Study-note section NET24

A /p IPv4 prefix has p leading one bits followed by 32-p zeros. Partial octet masks are 128,192,224,240,248,252,254. /19 is 255.255.224.0; /20 is 255.255.240.0; /21 is 255.255.248.0, correcting the study guide's 255.248.0.0 mistake.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 19 | lines 23-36

Classful addressing : In classful addressing, the addressspace is divided into five classes: A, B, C, D, and E.
• Netid and Hostid In classful addressing, an IP addressin class A, B, or C is divided into netid and hostid.
Subnetting: It allows a network to be split into several parts for internal use but still act like a single network to the outsideworld.
• To implement subnetting, the router needs a subnet mask that indicates the split between network + subnet number and host. Ex. 255.255.252.0/22. A‖/22‖ to indicate that the subnet mask is 22 bits long.

Data Communication and Computer Networking module | PDF page 19 | lines 2-22

Address Space: An address space is the total number ofaddresses used by the protocol.
• If a protocol uses N bits to define an address, the address space is 2N because each bit can have twodifferent values (0 or 1) and N bits can have 2N values.
• IPv4 uses 32-bit addresses, which means that the address space is 232 or 4,294,967,296 (more than 4billion).
Notations: There are two notations to show an IPv4 address:
• Binary notation: The IPv4 address is displayed as 32bits. ex. 11000001 10000011 00011011 11111111
• Dotted decimal notation: To make the IPv4 address easier to read, Internet addresses are usually written in decimal form with a decimal

point (dot) separatingthe bytes. Each byte (octet) is 8 bits hence each number in dotted-decimal notation is a value rangingfrom 0 to 255. Ex. 129.11.11.239

Question sources

Computer Science MCQ practice collection · Question 515

Question 212 | AM0516

How many bits are used for the host portion of an IP address with a subnet mask of 255.255.255.0?

A. 8 bits

B. 16 bits

C. 24 bits

D. 32 bits

Hint

Convert the mask to a prefix, separate network and host bits, and apply the relevant subnet-count or usable-host rule.

Answer A: 8 bits

255.255.255.0 contains 24 one bits and eight zero host bits. Subtract the 24-bit prefix from the 32-bit address width. Evidence: PDF 18, 19, 19.

Why each choice is right or wrong

A - Correct: Eight is 32-24 (PDF 18, 19, 19.)

B - Incorrect: Sixteen would require a /16 prefix (PDF 18, 19, 19.)

C - Incorrect: Twenty-four is the prefix count, not the host count (PDF 18, 19, 19.)

D - Incorrect: Thirty-two is the entire address width (PDF 18, 19, 19.)

Primary note proof

Study-note section NET24

A /p IPv4 prefix has p leading one bits followed by 32-p zeros. Partial octet masks are 128,192,224,240,248,252,254. /19 is 255.255.224.0; /20 is 255.255.240.0; /21 is 255.255.248.0, correcting the study guide’s 255.248.0.0 mistake.

Study-note section NET25

For ordinary broadcast LANs let h=32-p. Total addresses=2^h; usable hosts=2^h-2, reserving network and directed broadcast. Find the changing octet’s increment as 256-mask octet, round the address down to a multiple, and extend through the next boundary minus one.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 18 | lines 45-54

IP addresses: IP address uniquely identifies a device on the Internet. Every host and router on the Internet has an IP address, which encodes its network number and host number.
• The combination is unique: in principle, no two machines on the Internet have the same IP address.
• An IPv4 address is 32 bits long
• They are used in the Source address and Destination address fields of IP packets.
• An IP address does not refer to a host but it refers to a network interface.

Data Communication and Computer Networking module | PDF page 19 | lines 2-22

Address Space: An address space is the total number ofaddresses used by the protocol.
• If a protocol uses N bits to define an address, the address space is 2N because each bit can have twodifferent values (0 or 1) and N bits can have 2N values.
• IPv4 uses 32-bit addresses, which means that the address space is 232 or 4,294,967,296 (more than 4billion).
Notations: There are two notations to show an IPv4 address:
• Binary notation: The IPv4 address is displayed as 32bits. ex. 11000001 10000011 00011011 11111111
• Dotted decimal notation: To make the IPv4 address easier to read, Internet addresses are usually written in decimal form with a decimal point (dot) separatingthe bytes. Each byte (octet) is 8 bits hence each number in dotted-decimal notation is a value rangingfrom 0 to 255. Ex. 129.11.11.239

Data Communication and Computer Networking module | PDF page 19 | lines 23-36

Classful addressing : In classful addressing, the addressspace is divided into five classes: A, B, C, D, and E.
• Netid and Hostid In classful addressing, an IP addressin class A, B, or C is divided into netid and hostid.
Subnetting: It allows a network to be split into several parts for internal use but still act like a single network to

the outsideworld.
• To implement subnetting, the router needs a subnet mask that indicates the split between network + subnet number and host. Ex. 255.255.252.0/22. A‖/22‖ to indicate that the subnet mask is 22 bits long.

Question sources

Computer Science MCQ practice collection · Question 516

Question 213 | AM0517

Given a subnet mask of 255.255.255.224, how many host addresses are available in each subnet?

A. 6

B. 14

C. 30

D. 62

Hint

Convert the mask to a prefix, separate network and host bits, and apply the relevant subnet-count or usable-host rule.

Answer C: 30 host addresses per ordinary subnet

The mask 255.255.255.224 is /27, leaving five host bits. A block therefore contains 32 addresses. Because the question asks addresses available to hosts, exclude its network and broadcast addresses, leaving 30. Treating all 32 as usable would confuse block size with conventional broadcast-LAN host capacity.

Why each choice is right or wrong

A - Incorrect: Six usable addresses corresponds to /29, not the stated /27 mask.

B - Incorrect: Fourteen usable addresses corresponds to /28 and four host bits.

C - Correct: The /27 block has five host bits and 32−2=30 conventional usable addresses.

D - Incorrect: Sixty-two usable addresses would require /26 and six host bits.

Primary note proof

Study-note section NET25

For ordinary broadcast LANs let h=32-p. Total addresses=2^h; usable hosts=2^h-2, reserving network and directed broadcast. Find the changing octet’s increment as 256-mask octet, round the address down to a multiple, and extend through the next boundary minus one.

Study-note section NET24

A /p IPv4 prefix has p leading one bits followed by 32-p zeros. Partial octet masks are 128,192,224,240,248,252,254. /19 is 255.255.224.0; /20 is 255.255.240.0; /21 is 255.255.248.0, correcting the study guide’s 255.248.0.0 mistake.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 19 | lines 2-22

Address Space: An address space is the total
number ofaddresses used by the protocol.
• If a protocol uses N bits to define an address,
the address space is 2N
because each bit can
have twodifferent values (0 or 1) and N bits
can have 2N values.
• IPv4 uses 32-bit addresses, which means that
the address space is 232 or 4,294,967,296
(more than 4billion).
Notations: There are two notations to show an IPv4 address:
• Binary notation: The IPv4 address is displayed
as 32bits. ex. 11000001 10000011 00011011
11111111
• Dotted decimal notation: To make the IPv4
address easier to read, Internet addresses are
usually written in decimal form with a decimal
point (dot) separatingthe bytes. Each byte (octet)
is 8 bits hence each number in dotted-decimal
notation is a value rangingfrom 0 to 255. Ex.
129.11.11.239

Data Communication and Computer Networking module | PDF page 19 | lines 23-36

Classful addressing : In classful addressing, the
addressspace is divided into five classes: A, B, C,
D, and E.
• Netid and Hostid In classful addressing, an IP
addressin class A, B, or C is divided into netid
and hostid.
Subnetting: It allows a network to be split into several
parts for internal use but still act like a single network to
the outsideworld.
• To implement subnetting, the router needs a
subnet mask that indicates the split between
network + subnet number and host. Ex.
255.255.252.0/22. A‖/22‖ to indicate that the
subnet mask is 22 bits long.

Question sources

Computer Science MCQ practice collection · Question 517

Question 214 | AM0518

What is the network address for the IP address 192.168.1.65/26?

A. 192.168.1.0

B. 192.168.1.64

C. 192.168.1.65

D. 192.168.1.128

Hint

Convert the mask to a prefix, separate network and host bits, and apply the relevant subnet-count or usable-host rule.

Answer B: 192.168.1.64

/26 makes the fourth-octet mask192=11000000. 65=01000001 AND192=11000000 gives64=01000000, so the network is 192.168.1.64. Evidence: PDF 18, 19, 19.

Why each choice is right or wrong

A - Incorrect: 0 is the preceding 64-address block (PDF 18, 19, 19.)

B - Correct: 64 is the masked network boundary (PDF 18, 19, 19.)

C - Incorrect: 65 retains the nonzero host bit (PDF 18, 19, 19.)

D - Incorrect: 128 is the next block boundary (PDF 18, 19, 19.)

Primary note proof

Study-note section NET24

> Compute network=address AND mask. Host bits zero identify the block start; host bits one give broadcast. With 172.16.28.252/20, the third octet is grouped in blocks of 16, so the network is 172.16.16.0 and broadcast 172.16.31.255. A written host/prefix such as 172.105.180.0/21 need not be an aligned block label: masking yields 172.105.176.0/21.

Study-note section NET25

> For ordinary broadcast LANs let h=32-p. Total addresses=2^h; usable hosts=2^h-2, reserving network and directed broadcast. Find the changing octet's increment as 256-mask octet, round the address down to a multiple, and extend through the next boundary minus one.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 18 | lines 45-54

IP addresses: IP address uniquely identifies a device on the Internet. Every host and router on the Internet has an IP address, which encodes its network number and host number.
• The combination is unique: in principle, no two machines on the Internet have the same IP address.
• An IPv4 address is 32 bits long
• They are used in the Source address and Destination address fields of IP packets.
• An IP address does not refer to a host but it refers to a network interface.

Data Communication and Computer Networking module | PDF page 19 | lines 2-22

Address Space: An address space is the total number ofaddresses used by the protocol.
• If a protocol uses N bits to define an address, the address space is 2N because each bit can have twodifferent values (0 or 1) and N bits can have 2N values.
• IPv4 uses 32-bit addresses, which means that the address space is 232 or 4,294,967,296 (more than 4billion).
Notations: There are two notations to show an IPv4 address:
• Binary notation: The IPv4 address is displayed as 32bits. ex. 11000001 10000011 00011011 11111111
• Dotted decimal notation: To make the IPv4 address easier to read, Internet addresses are usually written in decimal form with a decimal point (dot) separatingthe bytes. Each byte (octet) is 8 bits hence each number in dotted-decimal notation is a value rangingfrom 0 to 255. Ex. 129.11.11.239

Data Communication and Computer Networking module | PDF page 19 | lines 23-36

Classful addressing : In classful addressing, the addressspace is divided into five classes: A, B, C, D, and E.
• Netid and Hostid In classful addressing, an IP addressin class A, B, or C is divided into netid and hostid.
Subnetting: It allows a network to be split into several parts for internal use but still act like a single network to the outsideworld.
• To implement subnetting, the router needs a subnet mask that indicates the split between network + subnet number and host. Ex.

255.255.252.0/22. A‖/22‖ to indicate that the subnet mask is 22 bits long.

Question sources

Computer Science MCQ practice collection · Question 518

Question 215 | AM0519

How many subnets can be created from a Class C network with a subnet mask of 255.255.255.192?

A. 2

B. 4

C. 8

D. 16

Hint

Convert the mask to a prefix, separate network and host bits, and apply the relevant subnet-count or usable-host rule.

Answer B: 4 subnets

A historical Class C parent is /24. The supplied 255.255.255.192 mask is /26, borrowing two bits. Modern counting gives 2^2=4 equal subnets, not two: NET26 explicitly rejects subtracting two subnets under modern practice. Here the parent is given, unlike the under-specified standalone-prefix questions.

Why each choice is right or wrong

A - Incorrect: Two would incorrectly exclude two subnets under an obsolete unstated convention; modern counting gives four.

B - Correct: Borrowing two bits from /24 to /26 produces four equal subnets.

C - Incorrect: Eight subnets requires borrowing three bits, producing /27 rather than /26.

D - Incorrect: Sixteen subnets requires four borrowed bits and a /28 prefix.

Primary note proof

Study-note section NET26

To split parent /a into equal /p blocks, borrow b=p-a bits and obtain 2^b subnets. Do not subtract two subnets under modern practice. For a Class B /16 parent split to /19, b=3 gives eight subnets, each with 8192 addresses and 8190 conventional hosts. A /19 alone does not state its parent.

Study-note section NET22

Historical classes use leading patterns: A 0 with /8, B 10 with /16, C 110 with /24; D 1110 is multicast and E 1111 reserved. Ordinary class-A first octets are 1-126 because 0 and 127 have

special uses. B spans 128-191 and C 192-223. Default usable counts are 2^24-2, 2^16-2 and 254. Modern CIDR requires the actual prefix and overrides class defaults.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 19 | lines 2-22

Address Space: An address space is the total
number ofaddresses used by the protocol.
• If a protocol uses N bits to define an address,
the address space is 2N
because each bit can
have twodifferent values (0 or 1) and N bits
can have 2N values.
• IPv4 uses 32-bit addresses, which means that
the address space is 232 or 4,294,967,296
(more than 4billion).
Notations: There are two notations to show an IPv4 address:
• Binary notation: The IPv4 address is displayed
as 32bits. ex. 11000001 10000011 00011011
11111111
• Dotted decimal notation: To make the IPv4
address easier to read, Internet addresses are
usually written in decimal form with a decimal
point (dot) separatingthe bytes. Each byte (octet)
is 8 bits hence each number in dotted-decimal
notation is a value rangingfrom 0 to 255. Ex.
129.11.11.239

Data Communication and Computer Networking module | PDF page 19 | lines 23-36

Classful addressing : In classful addressing, the
addressspace is divided into five classes: A, B, C,
D, and E.
• Netid and Hostid In classful addressing, an IP
addressin class A, B, or C is divided into netid
and hostid.
Subnetting: It allows a network to be split into several
parts for internal use but still act like a single network to
the outsideworld.
• To implement subnetting, the router needs a
subnet mask that indicates the split between
network + subnet number and host. Ex.
255.255.252.0/22. A‖/22‖ to indicate that the
subnet mask is 22 bits long.

Data Communication and Computer Networking module | PDF page 19 | lines 37-44

CIDR: A class B address is far too large for most organizationsand a class C network, with 256 addresses is too small. This leads to granting Class B address to organizations who do not require all. This is resulting in depletion of Address space. A solution is CIDR (Classless InterDomain Routing) The basic idea behind CIDR, is to allocate the remaining IP addresses in variable-sized blocks, without regard to the classes.

Question sources

Computer Science MCQ practice collection · Question 519

Question 216 | AM0520

What is the maximum number of IP addresses that can be assigned to hosts in a subnet with a /27 subnet mask?

A. 14

B. 30

C. 62

D. 126

Hint

Convert the mask to a prefix, separate network and host bits, and apply the relevant subnet-count or usable-host rule.

Answer B: 30 assignable host IP addresses

With /27, 32−27=5 host bits produce 2^5=32 addresses. For an ordinary subnet, network and broadcast are reserved, so 30 can be assigned to hosts. The alternative values are usable-host counts for /28, /26 and /25, rather than the supplied /27.

Why each choice is right or wrong

A - Incorrect: Fourteen usable hosts requires /28, leaving only four host bits.

B - Correct: A /27 leaves five host bits and therefore 30 assignable ordinary host addresses.

C - Incorrect: Sixty-two usable hosts is the /26 result, not /27.

D - Incorrect: 126 usable hosts requires /25 and seven host bits.

Primary note proof

Study-note section NET25

For ordinary broadcast LANs let h=32-p. Total addresses=2^h; usable hosts=2^h-2, reserving network and directed broadcast. Find the changing octet’s increment as 256-mask octet, round the address down to a multiple, and extend through the next boundary minus one.

Study-note section NET24

A /p IPv4 prefix has p leading one bits followed by 32-p zeros. Partial octet masks are 128,192,224,240,248,252,254. /19 is 255.255.224.0; /20 is 255.255.240.0; /21 is 255.255.248.0, correcting the study guide's 255.248.0.0 mistake.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 18 | lines 45-54

IP addresses: IP address uniquely identifies a device on the
Internet. Every host and router on the Internet has an IP address,
which encodes its network number and host number.
• The combination is unique: in principle, no two
machines on the Internet have the same IP address.
• An IPv4 address is 32 bits long
• They are used in the Source address and Destination
address fields of IP packets.
• An IP address does not refer to a host but it refers to a
network interface.

Data Communication and Computer Networking module | PDF page 19 | lines 2-22

Address Space: An address space is the total
number ofaddresses used by the protocol.
• If a protocol uses N bits to define an address,
the address space is 2N
because each bit can
have twodifferent values (0 or 1) and N bits
can have 2N values.
• IPv4 uses 32-bit addresses, which means that
the address space is 232 or 4,294,967,296
(more than 4billion).
Notations: There are two notations to show an IPv4 address:
• Binary notation: The IPv4 address is displayed
as 32bits. ex. 11000001 10000011 00011011
11111111
• Dotted decimal notation: To make the IPv4
address easier to read, Internet addresses are
usually written in decimal form with a decimal
point (dot) separatingthe bytes. Each byte (octet)
is 8 bits hence each number in dotted-decimal
notation is a value rangingfrom 0 to 255. Ex.
129.11.11.239

Data Communication and Computer Networking module | PDF page 19 | lines 23-36

Classful addressing : In classful addressing, the
addressspace is divided into five classes: A, B, C,
D, and E.

• Netid and Hostid In classful addressing, an IP addressin class A, B, or C is divided into netid and hostid.
Subnetting: It allows a network to be split into several parts for internal use but still act like a single network to the outsideworld.
• To implement subnetting, the router needs a subnet mask that indicates the split between network + subnet number and host. Ex. 255.255.252.0/22. A‖/22‖ to indicate that the subnet mask is 22 bits long.

Question sources

Computer Science MCQ practice collection · Question 520

Question 217 | AM0521

Which IP address range is reserved for Automatic Private IP Addressing (APIPA)?

A. 10.0.0.0 - 10.255.255.255

B. 127.0.0.0 - 127.255.255.255

C. 169.254.0.0 - 169.254.255.255

D. 192.168.0.0 - 192.168.255.255

Hint

Separate address width, syntax, reserved scope and the supplied prefix or historical classful convention.

Answer C: 169.254.0.0/16 link-local/APIPA range

NET23 assigns link-local/APIPA to 169.254.0.0/16, the range printed in C. That identifies the reserved overall block; the first and last /24 blocks are excluded from normal automatic selection. The private RFC1918 blocks and loopback block offered elsewhere have different purposes and are not the APIPA range.

Why each choice is right or wrong

A - Incorrect: 10/8 is RFC1918 private space, not the link-local/APIPA allocation.

B - Incorrect: 127/8 is loopback for local protocol access, not automatic link-local addressing.

C - Correct: 169.254/16 is the APIPA block; normal automatic host selection excludes its edge /24 blocks.

D - Incorrect: 192.168/16 is RFC1918 private space rather than the APIPA block.

Primary note proof

Study-note section NET23

RFC1918 private blocks are 10.0.0.0/8, 172.16.0.0/12 (through 172.31.255.255), and 192.168.0.0/16. They can be reused internally but are not globally routed as public destinations. A LAN may also use legitimately assigned public addresses; private is common, not mandatory. 127.0.0.0/8 is IPv4 loopback, commonly 127.0.0.1, for local protocol access without an external link. 255.255.255.255 is limited broadcast; 0.0.0.0 can identify an unconfigured source. Link-local/APIPA uses 169.254.0.0/16, with edge /24 blocks excluded from normal automatic selection.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 19 | lines 45-49

NAT (Network Address Translation): The scarcity of
network addresses in IPv4 led to the development of IPv6.
Due to this, we need to use private IP address inside the
organization and translate it to public IP address using
NAT.

Data Communication and Computer Networking module | PDF page 65 | lines 31-38

/etc/hosts
The /etc/hosts file always contains the localhost IP
address, 127.0.0.1, which is
usedfor interprocess communication.
Never remove this line! Sometimes contains
addresses of additional hosts, whichcan be contacted
without using an external naming service such as
DNS (the Domain Name Server).

Data Communication and Computer Networking module | PDF page 19 | lines 2-22

Address Space: An address space is the total
number ofaddresses used by the protocol.
• If a protocol uses N bits to define an address,
the address space is 2N
because each bit can
have twodifferent values (0 or 1) and N bits
can have 2N values.
• IPv4 uses 32-bit addresses, which means that
the address space is 232 or 4,294,967,296
(more than 4billion).
Notations: There are two notations to show an IPv4 address:
• Binary notation: The IPv4 address is displayed
as 32bits. ex. 11000001 10000011 00011011
11111111
• Dotted decimal notation: To make the IPv4
address easier to read, Internet addresses are
usually written in decimal form with a decimal
point (dot) separatingthe bytes. Each byte (octet)
is 8 bits hence each number in dotted-decimal

notation is a value rangingfrom 0 to 255. Ex.
129.11.11.239

Question sources

Computer Science MCQ practice collection · Question 521

Question 218 | AM0523

Which of the following protocols is responsible for assigning IP addresses to hosts dynamically?

A. DNS

B. DHCP

C. HTTP

D. FTP

Hint

Identify the requested service or delivery guarantee, then distinguish application roles, transport behavior and address configuration.

Answer B: DHCP

DHCP is the address-configuration service in NET20, dynamically leasing an address together with other settings. DNS resolves names rather than assigning a client's host address. HTTP and FTP handle web exchanges and file transfers. Therefore B matches dynamic assignment rather than name resolution or application-data transfer.

Why each choice is right or wrong

A - Incorrect: DNS resolves names to records and does not perform the dynamic lease assignment asked about.

B - Correct: DHCP dynamically leases host addresses and related network configuration.

C - Incorrect: HTTP provides web request/response exchanges rather than dynamic IP-address allocation.

D - Incorrect: FTP transfers files and is not a host-address lease protocol.

Primary note proof

Study-note section NET20

DNS resolves names to records, including IPv4 A and IPv6 AAAA addresses; it can use UDP or TCP port 53. DHCP dynamically leases IPv4 settings, commonly address, mask, gateway and DNS server. Its basic exchange is discover, offer, request, acknowledge. IP itself does not assign addresses.

Study-note section NET21

HTTP defines web request/response semantics; it is stateless, and a message body may be absent. HTTPS adds TLS protection. FTP transfers files using control and separate data connections; it is not the same protocol as SFTP. SMTP submits and relays mail; POP3 retrieves messages and IMAP accesses/synchronizes server mailboxes. Saying SMTP handles both sending and end-user mailbox retrieval is inaccurate.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 28 | lines 32-45

Application Layer
The application layer in TCP/IP is equivalent to the combined session, presentation, and application layers in the OSI model and many protocols are defined at this layer.
The Process/Application Layer Protocols
• Telnet
• File Transfer Protocol (FTP)
• Network File System (NFS).
• Simple Mail Transfer Protocol (SMTP
• POP3 is used to receive mail.
• Simple Network Management Protocol (SNMP)
• Domain Name Service (DNS)
• Dynamic Host Configuration Protocol (DHCP)

Data Communication and Computer Networking module | PDF page 18 | lines 27-32

Application Layer
The Application Layer is a combination of Session, Presentation & Application Layers of OSI models and defines high level protocols like File Transfer (FTP), Electronic Mail (SMTP), Virtual Terminal (TELNET), Domain Name Service (DNS), etc.

Question sources

Computer Science MCQ practice collection · Question 523

Question 219 | CS0155

Which TCP/IP-suite protocols listed below are connectionless? Select all that apply.

A. User Datagram Protocol (UDP)

B. Internet Protocol

C. Transmission Control Protocol

D. The OSI reference protocol

Hint

Identify the requested service or delivery guarantee, then distinguish application roles, transport behavior and address configuration.

Answer A, B: User Datagram Protocol (UDP); Internet Protocol

UDP sends independent datagrams without built-in connection setup, ordering or retransmission. IP likewise provides connectionless best-effort packet delivery at the network layer. TCP instead establishes transport connection state and supplies a reliable ordered stream. OSI is a reference model rather than a protocol in the TCP/IP suite. The multiple-selection instruction therefore permits both connectionless protocols across the two layers.

Why each choice is right or wrong

A - Correct: UDP has no built-in connection setup and treats datagrams independently.

B - Correct: IP also supplies connectionless best-effort packet delivery at the network layer.

C - Incorrect: TCP establishes logical transport connection state before its reliable stream transfer.

D - Incorrect: OSI is a reference model, not a connectionless TCP/IP-suite protocol.

Primary note proof

Study-note section NET17

> TCP offers a reliable ordered byte stream using sequence numbers, acknowledgments, retransmission and windows. Flow control protects the receiver; congestion control protects network capacity. UDP sends independent datagrams with ports and a checksum but no built-in setup, delivery guarantee, retransmission or ordering. Live interactive traffic may choose UDP when late data is less useful than lost data. Application protocols can add reliability over UDP.

Study-note section NET16

> IP supplies connectionless best-effort packet delivery, not end-to-end ordering or retransmission. IPv4 addresses are 32 bits. Its minimum header is 20 bytes and can grow to 60 bytes; it is not a 32-bit header. IHL counts 32-bit words; total length includes header and payload. TTL limits lifetime across routers; the protocol field identifies TCP, UDP or another upper-layer protocol.

Study-note section NET03

> A reference model divides responsibilities and interfaces; it is not itself executable networking software. OSI is a seven-layer reference model; TCP/IP describes an implemented protocol suite, usually taught with four layers. A five-layer teaching model separates physical and link functions. State the model before counting layers.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 18 | lines 9-21

> TCP - Transmission Control Protocol: TCP is a reliable
> connection-oriented, reliable protocol. i.e. a connection is
> established between the sender and receiver before the data can

be transmitted. It divides the data it receives from the upper layer into segments and tags a sequence number to each segment which is used at the receiving end for reordering of data.
UDP - User Datagram Protocol: UDP is a simple protocol used for process to process transmission. It is an unreliable, connectionless protocol for applications that do not require flow control or error control. It simply adds port address, checksum and length information to the data it receives from the upper layer.

Data Communication and Computer Networking module | PDF page 17 | lines 22-38

Network Layer or IP
Also called as the Internetwork Layer (IP). It holds the IP protocol which is a network layer protocol and is responsiblefor source to destination transmission of data.
The Internetworking Protocol (IP) is a connection-less & unreliable protocol.
It is a best effort delivery service. i.e. there is no error checking in IP, it simply sends the data and relies on its underlying layers to get the data transmitted to the destination.Even if it is unreliable IP cannot be considered weak and useless; since it provides only the functionality that is requiredfor transmitting data thereby giving maximum efficiency.
Since there is no mechanism of error detection or correction in IP, there will be no delay introduced on a medium where thereis no error at all.

Data Communication and Computer Networking module | PDF page 14 | lines 12-29

The Open Systems Interconnection (OSI) Model was developed by International Organization for Standardization (ISO). ISO is the organization, OSI is the model
It was developed to allow systems with different platforms (Hardware & software) to communicate with each other.
Now, it is a network model that defines the protocols for network communications.
It is a hierarchical model that groups its processes into seven (7) layers. (Top to Bottom)
1. Application Layer
2. Presentation Layer
3. Session Layer
4. Transport Layer
5. Network Layer
6. Data Link Layer

7. Physical Layer
Each layer has specific functions to perform and has to co-operate with the layers above and below it.

Question sources

Computer Science Exit Exam practice collection · Question 155

Question 220 | CS0156

Which statements describe capabilities or properties of IPv6? Select all that apply. Encryption support in D means capability, not automatic confidentiality or exclusivity to IPv6.

A. Handle more addresses

B. Use 128-bits

C. Route slower and is memory intensive

D. Support encryptions

Hint

Identify the requested service or delivery guarantee, then distinguish application roles, transport behavior and address configuration.

Answer A, B, D: Handle more addresses; Use 128-bits; Support encryptions

IPv6 uses 128-bit addresses, giving it a much larger address space than IPv4's 32-bit addresses. It can support encryption, but that capability does not mean every IPv6 packet is encrypted or that IPv4 cannot support encryption. Routing speed and memory requirements depend on implementation and workload; they are not inherently fixed by the protocol version. Thus the three capability/property statements qualify.

Why each choice is right or wrong

A - Correct: A 128-bit address space can represent far more addresses than IPv4's 32-bit space.

B - Correct: NET23 explicitly states that IPv6 addresses contain 128 bits.

C - Incorrect: Slower routing and greater memory use are not inherent requirements of every IPv6 implementation.

D - Correct: Encryption is supported, but IPv6 does not automatically encrypt traffic and this is not unique to IPv6.

Primary note proof

Study-note section NET23

IPv6 has 128-bit hexadecimal addresses, flexible prefixes and no IPv4-style broadcast. Sources, not routers, fragment IPv6 packets. IPv6 does not automatically encrypt traffic or make authentication unnecessary. Compare IPv6's larger 128-bit address space and encryption support separately; specify the property being evaluated.

Study-note section NET16

IP supplies connectionless best-effort packet delivery, not end-to-end ordering or retransmission. IPv4 addresses are 32 bits. Its minimum header is 20 bytes and can grow to 60 bytes; it is not a 32-bit header. IHL counts 32-bit words; total length includes header and payload. TTL limits lifetime across routers; the protocol field identifies TCP, UDP or another upper-layer protocol.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 18 | lines 45-54

IP addresses: IP address uniquely identifies a device on the
Internet. Every host and router on the Internet has an IP address,
which encodes its network number and host number.
• The combination is unique: in principle, no two
machines on the Internet have the same IP address.
• An IPv4 address is 32 bits long
• They are used in the Source address and Destination
address fields of IP packets.
• An IP address does not refer to a host but it refers to a
network interface.

Data Communication and Computer Networking module | PDF page 19 | lines 45-49

NAT (Network Address Translation): The scarcity of
network addresses in IPv4 led to the development of IPv6.
Due to this, we need to use private IP address inside the
organization and translate it to public IP address using
NAT.

Question sources

Computer Science Exit Exam practice collection · Question 156

Question 221 | CS0157

Which one does NOT describe a loopback address?

A. It helps to refer to the host itself

B. It allows programs to access network protocols for local services

C. It is an external pseudo address

D. It is denoted by the IP address: 127.0.0.1

Hint

Separate address width, syntax, reserved scope and the supplied prefix or historical classful convention.

Answer C: Loopback is local self-reference, not an external address

Loopback lets a host address itself and access local services through networking protocols without an external link. NET23 identifies 127/8 and common 127.0.0.1 for that purpose. Describing it as external contradicts this local scope, whereas the remaining choices all describe supported loopback uses or notation.

Why each choice is right or wrong

A - Incorrect: Referring to the host itself is precisely the loopback function, so this statement does describe it.

B - Incorrect: Local programs can use networking protocols to access local services through loopback.

C - Correct: External contradicts loopback's local self-reference without an external network link.

D - Incorrect: 127.0.0.1 is explicitly given as the common IPv4 loopback address.

Primary note proof

Study-note section NET23

> RFC1918 private blocks are 10.0.0.0/8, 172.16.0.0/12 (through 172.31.255.255), and 192.168.0.0/16. They can be reused internally but are not globally routed as public destinations. A LAN may also use legitimately assigned public addresses; private is common, not mandatory. 127.0.0.0/8 is IPv4 loopback, commonly 127.0.0.1, for local protocol access without an external link. 255.255.255.255 is limited broadcast; 0.0.0.0 can identify an unconfigured source. Link-local/APIPA uses 169.254.0.0/16, with edge /24 blocks excluded from normal automatic selection.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 65 | lines 31-38

> /etc/hosts
> The /etc/hosts file always contains the localhost IP
> address, 127.0.0.1, which is
> usedfor interprocess communication.
> Never remove this line! Sometimes contains
> addresses of additional hosts, whichcan be contacted
> without using an external naming service such as
> DNS (the Domain Name Server).

Question sources

Computer Science Exit Exam practice collection · Question 157

Question 222 | CS0164

In data communication, which of the following is NOT a factor for data rate?

A. Travel distance

B. Bandwidth available

C. Level of noise

D. Levels of the signals

Hint

Use the cited note definitions to identify the requested function or scope, then check each alternative against that same rule.

Answer A: Travel distance is not explicit in the simplified capacity formulas

In the simplified capacity comparison taught in NET05, Nyquist uses bandwidth and signal levels, while Shannon uses bandwidth and signal-to-noise ratio. Travel distance is not a separate formula parameter, making A the intended choice. The qualification matters: distance can affect attenuation, delay and real achievable rates, so the answer is not physical independence from distance.

Why each choice is right or wrong

A - Correct: Travel distance is absent as an independent variable in the taught formulas, despite indirect real-link effects.

B - Incorrect: Bandwidth appears directly in both Nyquist and Shannon expressions and limits channel capacity.

C - Incorrect: Noise enters Shannon capacity through the signal-to-noise ratio.

D - Incorrect: Signal levels enter Nyquist capacity through the number of bits represented per symbol.

Primary note proof

Study-note section NET05

> For an ideal noiseless channel, Nyquist gives $R \leq 2B \log_2(M)$. For Gaussian noise, Shannon gives $C = B \log_2(1+S/N)$, with a linear power ratio; $SNR(dB) = 10 \log_{10}(S/N)$. Bandwidth, signal levels and noise appear explicitly. Distance affects attenuation, delay and often achievable rate, but is not a separate variable in these simplified capacity formulas.

Study-note section NET06

> Transmission delay is packet bits divided by link bit rate; propagation delay is distance divided by signal speed. Processing and queueing add delay. A 1000-byte packet takes 0.8 ms to serialize at 10 Mbit/s; increasing line rate does not reduce propagation time.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 9 | lines 2-14

BIT LENGTH or Bit Interval (Tb)
It is the time required to send one bit.
It is measured in seconds.
BIT RATE
It is the number of bits transmitted in one second.
It is expressed as bits per second (bps).
Relation between bit rate and bit interval can be as follows
Bit rate = 1 / Bit interval
Baud Rate
It is the rate of Signal Speed, i.e the rate at which the signal changes.
A digital signal with two levels 0_& 1_will have the same baud rate and bit rate & bit rate.

Data Communication and Computer Networking module | PDF page 10 | lines 18-35

receiver.There are three causes of impairment:
• Attenuation
• Distortion
• Noise
Attenuation
Attenuation results in loss of energy due to distance.
Whena signal travels through a medium, it loses some of its energy in overcoming the resistance of the medium. The electrical energy in the signal may convert to heat. To compensate for this loss, amplifiers are used to amplify thesignal.
Distortion
Distortion changes the shape of the signal.
Noise
Noise is any unwanted signal that is mixed or combined with the original signal during transmission.
Due to noise the original signal is altered and signal received is not sameas the one sent.

Data Communication and Computer Networking module | PDF page 9 | lines 29-49

Transmission of Digital signal: Digital signal can be transmitted in the following two ways:
• Baseband Transmission: The signal is transmitted without making any change to it (i.e. Without modulation)
o In baseband transmission, the bandwidth of the signal to be transmitted has to be less than the bandwidth of the channel.
o Ex. Consider a Baseband channel with lower frequency 0Hz and higher frequency 100Hz, hence its bandwidth is 100 (Bandwidth is calculated by getting the difference between the highest and lowest frequency)
o A channel whose bandwidth is more than the bandwidth

of the signal is called Wideband channel
o A channel whose bandwidth is less than the bandwidth of the signal is called Narrowband channel
• Broadband Transmission: Given a bandpass channel, a digital signal cannot be transmitted directly through it
o In broadband transmission we use modulation, i.e. we change the signal to analog signal before transmitting it.

Question sources

Computer Science Exit Exam practice collection · Question 164

Question 223 | NS0334

Which of the following OSI layers is NOT correctly matched to its corresponding data Units (PDU)?

A. Application layer ---> Data

B. Transport layer ---> Segment

C. Physical layer ---> Bit

D. Network layer ---> Frame

Hint

Match the requested scope or data unit to the layer duties in the note; distinguish hop delivery from end-to-end process delivery.

Answer D: Network-layer PDU is packet, not frame

The PDUs are: application data, transport segment/datagram, network packet, link frame and physical bits. D assigns the link-layer frame to the network layer, making it the mismatch. Transport segment is appropriate for TCP, so B remains a valid conventional example rather than a claim about every transport protocol.

Why each choice is right or wrong

A - Incorrect: Application data is the conventional PDU designation, so this match is valid.

B - Incorrect: TCP uses transport segments; this is a valid conventional transport PDU example.

C - Incorrect: Bits/symbols belong to physical transport, making this match valid.

D - Correct: A frame is link-layer; the network-layer unit is a packet.

Primary note proof

Study-note section NET12

> Sending proceeds from application data to transport segment/datagram, network packet, link frame and physical bits/symbols; receiving reverses the order. Each layer serves the layer above. A router removes a received link frame, inspects IP, and creates a new link frame for the next hop. MAC addresses usually change across routed hops; end-to-end IP addresses ordinarily remain until translation.

Question sources

Computer Science Exit Exam · 2018 · Question 63

Question 224 | NS0341

Which of the following layers is responsible for encryption, translation and compression?

A. Presentation layer

B. Data link layer

C. Transport layer

D. Network layer

Hint

Match the requested scope or data unit to the layer duties in the note; distinguish hop delivery from end-to-end process delivery.

Answer A: Presentation layer

The three listed operations are representation functions: encoding translation, compression and encryption. NET19 groups them under the OSI presentation role. Link handles frames, transport process delivery and network logical routing; none is the named OSI representation layer. Real implementations may distribute these functions, but the reference-model answer is presentation.

Why each choice is right or wrong

A - Correct: Presentation explicitly covers encoding translation, compression and encryption roles.

B - Incorrect: Data link handles hop frames/access rather than the OSI representation-function grouping.

C - Incorrect: Transport delivers between process endpoints, not the named presentation representation roles.

D - Incorrect: Network handles logical addressing/routing rather than compression/encoding translation.

Primary note proof

Study-note section NET19

> OSI session roles establish/manage dialogs and can coordinate checkpoints so transfer resumes after interruption. Presentation roles translate encodings and handle compression/encryption. Compression reduces representation size; encryption hides content and need not shrink it. Application protocols provide services directly to applications. Practical implementations distribute these functions differently; TLS is not proof of a separate physical presentation-layer device.

Study-note section NET12

> Sending proceeds from application data to transport segment/datagram, network packet, link frame and physical bits/symbols; receiving reverses the order. Each layer serves the layer above. A router removes a received link frame, inspects IP, and creates a new link frame for the next hop. MAC addresses usually change across routed hops; end-to-end IP addresses ordinarily remain until translation.

Question sources

Computer Science Exit Exam · 2018 · Question 72

Question 225 | NS0352

Assume that you have IPv4 addresses in binary notation 11000001 10000011 00011011 11111111 and you are requested to change into dotted decimal notation. What is the equivalent IP address in decimal dotted notation?

A. 192.174.27.255

B. 192.134.67.254

C. 193.130.28.254

D. 193.131.27.255

Hint

Sum the eight bit weights in each octet independently, then preserve their order in dotted-decimal notation.

Answer D: 193.131.27.255

Using octet weights 128,64,32,16,8,4,2,1 gives 11000001=193, 10000011=131, 00011011=27 and 11111111=255. Combining the four decimal octets gives 193.131.27.255. This is a notation conversion, not a claim about whether that address is assignable as a host under an unspecified prefix.

Why each choice is right or wrong

A - Incorrect: The first octet should be 193 and the second 131, not 192 and 174.

B - Incorrect: All four printed octets differ from the binary-derived values 193,131,27,255.

C - Incorrect: Only the first octet matches; the correct remaining values are 131,27,255.

D - Correct: Each decimal octet matches its eight-bit sum: 193, 131, 27 and 255.

Primary note proof

Study-note section NET22

> Write IPv4 as four decimal octets 0-255, or as 32 binary bits. Use weights 128,64,32,16,8,4,2,1 within each octet. Thus 11000001 10000011 00011011 11111111 is 193.131.27.255. A value such as 257 is impossible. Syntactic validity differs from assignability: an address ending .0 or .255 can be a host under some prefixes.

Question sources

Computer Science Exit Exam · 2018 · Question 89

Question 226 | NS0573

A company has 500 computers distributed across 10 floors of a single building. Which network type BEST describes this setup?

A. WAN

B. MAN

C. LAN

D. Internet

Hint

Use the cited note definitions to identify the requested function or scope, then check each alternative against that same rule.

Answer C: LAN

All computers are in one building, the geographic scope of a LAN in NET02. The count of 500 devices or ten floors does not itself make a MAN/WAN; the note explicitly separates device count from geographic category. No metropolitan or distant-region interconnection is supplied.

Why each choice is right or wrong

A - Incorrect: WAN concerns distant regions, not simply many devices on floors of one building.

B - Incorrect: MAN requires metropolitan scope rather than a single-building deployment.

C - Correct: A single building falls within the LAN scope defined by NET02.

D - Incorrect: The Internet is the global network of networks, not the building network described.

Primary note proof

Study-note section NET02

> PAN connects personal devices, such as Bluetooth accessories. LAN covers a local building or campus; MAN spans a metropolitan region; WAN connects distant regions. Device count alone does not determine the category. The Internet is a global network of networks, commonly the largest example of a WAN.

Question sources

Data Communication & Networking review questions · Question 1

Question 227 | NS0574

In which OSI layer does the MAC address operate?

A. Network Layer (Layer 3)

B. Physical Layer (Layer 1)

C. Data Link Layer (Layer 2)

D. Transport Layer (Layer 4)

Hint

Match the requested scope or data unit to the layer duties in the note; distinguish hop delivery from end-to-end process delivery.

Answer C: Data link, layer 2

MAC addressing identifies link-layer frame endpoints and forwarding scope. NET13 assigns medium-dependent addressing/access to MAC in the data-link layer. Physical transports signals, network uses logical IP prefixes and transport identifies process endpoints by ports. The word physical in physical address must not be confused with a layer-1 functional assignment.

Why each choice is right or wrong

A - Incorrect: Network-layer addressing uses logical IP addresses rather than the link MAC address.

B - Incorrect: Physical transports signals; the conventional physical-address nickname does not move MAC addressing to layer 1.

C - Correct: MAC addressing and frame delivery are data-link functions at layer 2.

D - Incorrect: Transport identifies process endpoints by ports rather than MAC frame addresses.

Primary note proof

Study-note section NET13

> Link-layer LLC identifies or multiplexes upper-layer protocols and may supply link control; MAC handles medium-dependent addressing/access and frame delivery. Network addressing belongs to layer 3. Ethernet, PPP and HDLC are link protocols. Frame headers may carry addresses and control/type fields; synchronization and exact framing depend on the protocol.

Study-note section NET17

> Ports identify transport endpoints; the application can choose a transport and request socket buffer sizes, subject to OS limits. A TCP connection is identified by source/destination IP and source/destination port, with TCP understood. IPv4 protocol numbers identify upper protocols; 80 is a usual HTTP port, not an IP protocol number. Clients often use ephemeral ports. SCTP is a reliable message-oriented transport with multiple streams.

Study-note section NET16

> IP supplies connectionless best-effort packet delivery, not end-to-end ordering or retransmission. IPv4 addresses are 32 bits. Its minimum header is 20 bytes and can grow to 60 bytes; it is not a 32-bit header. IHL counts 32-bit words; total length includes header and payload. TTL limits lifetime across routers; the protocol field identifies TCP, UDP or another upper-layer protocol.

Question sources

Data Communication & Networking review questions · Question 2

Question 228 | NS0575

Which of the following correctly describes attenuation in data transmission?

A. The delay caused by different frequencies traveling at different speeds

B. The loss of signal strength as it travels over a distance

C. Interference from adjacent communication channels

D. The maximum data rate of a transmission medium

Hint

Compare the signal mechanism, medium properties or transmission direction against the definitions and stated physical assumptions.

Answer B: Loss of signal strength

NET06 defines attenuation as reduced signal strength. Different delays among frequency components describe distortion, adjacent-channel leakage describes crosstalk and maximum rate concerns capacity. B gives the strength-loss mechanism rather than those separate impairments or performance measures.

Why each choice is right or wrong

A - Incorrect: Different component delays change waveform shape, describing distortion rather than attenuation.

B - Correct: A reduction in signal strength during propagation is attenuation.

C - Incorrect: Adjacent-channel interference is crosstalk, a separate noise source.

D - Incorrect: Maximum data rate is channel capacity, not signal-strength loss.

Primary note proof

Study-note section NET06

> Attenuation reduces signal strength. Distortion changes shape, often because frequencies have different delays. Noise adds unwanted energy: thermal noise comes from random thermal motion, crosstalk leaks from nearby channels, and impulse noise is a short disturbance. Amplifiers amplify noise too; digital repeaters regenerate decisions but cannot reconstruct every corrupted bit.

Study-note section NET05

> For an ideal noiseless channel, Nyquist gives $R \leq 2B \log_2(M)$. For Gaussian noise, Shannon gives $C = B \log_2(1+S/N)$, with a linear power ratio; $SNR(dB) = 10 \log_{10}(S/N)$. Bandwidth, signal levels and noise appear explicitly. Distance affects attenuation, delay and often achievable rate, but is not a separate variable in these simplified capacity formulas.

Question sources

Data Communication & Networking review questions · Question 3

Question 229 | NS0576

A network administrator wants to divide the Class C network 192.168.10.0 into 6 subnets. What is the minimum number of bits that must be borrowed from the host portion?

A. 2 bits

B. 3 bits

C. 4 bits

D. 6 bits

Hint

Convert the mask to a prefix, separate network and host bits, and apply the relevant subnet-count or usable-host rule.

Answer B: Borrow 3 bits to obtain at least six equal subnets

For equal-sized subnets of a /24 parent, borrowing b bits yields 2^b blocks. Two bits give only four; three give eight, the minimum power-of-two count that accommodates six required subnets. The resulting mask is /27 with 30 conventional hosts per block. Exactly six equal blocks would not fill the parent; two blocks remain unused.

Why each choice is right or wrong

A - Incorrect: Two borrowed bits yield only four blocks, fewer than the six required.

B - Correct: Three borrowed bits yield eight blocks and are the minimum satisfying at least six.

C - Incorrect: Four bits yield sixteen blocks and are not the minimum required.

D - Incorrect: Six bits yield sixty-four blocks, substantially more than the minimum.

Primary note proof

Study-note section NET26

> To split parent /a into equal /p blocks, borrow b=p-a bits and obtain 2^b subnets. Do not subtract two subnets under modern practice. For a Class B /16 parent split to /19, b=3 gives eight subnets, each with 8192 addresses and 8190 conventional hosts. A /19 alone does not state its parent.

Study-note section NET26

> For H hosts, choose the smallest h satisfying 2^h-2≥H, then p=32-h. For 24 hosts use /27; 52 or 57 use /26; 100 use /25; 500 use /23. For at least six equal subnets choose b=3. A Class C /24 split to /27 yields eight subnets. Always check both the number of subnets and the host capacity.

Question sources

Data Communication & Networking review questions · Question 4

Question 230 | NS0577

Which topology provides the HIGHEST level of redundancy?

A. Star

B. Ring

C. Bus

D. Mesh

Hint

Draw the links and identify shared components, alternate paths and the effect of the specified failure or growth requirement.

Answer D: Full mesh among the conventional topology choices

A full mesh connects every pair of nodes, offering multiple alternate paths compared with the basic star, single ring and shared bus. NET08 explains the additional links/interfaces and improved fault tolerance. D assumes the conventional full-mesh interpretation; actual protected rings or partial mesh designs would require more detail for a quantitative comparison.

Why each choice is right or wrong

A - Incorrect: A basic star depends on its central device and lacks the full mesh's many alternate paths.

B - Incorrect: A basic single ring is vulnerable to a break, unlike a full mesh's multiple paths.

C - Incorrect: A shared bus depends on one backbone rather than redundant pairwise paths.

D - Correct: A full mesh supplies pairwise links and multiple alternate paths, at increased cable/interface cost.

Primary note proof

Study-note section NET08

> Bus uses a shared backbone; an unterminated break can disrupt the segment. Star connects endpoints through a central device: one edge failure isolates that endpoint, whereas central failure affects the star. Ring forms a loop; basic single rings are vulnerable to a break, while protected dual rings differ. Token passing is associated with Token Ring but is an access method, not a necessary property of every ring. Tree is hierarchical; hybrid combines arrangements.

Study-note section NET08

> A full undirected mesh of n nodes needs n(n-1)/2 links and n-1 interfaces per node. For 50 nodes: 50×49/2=1225 links. Redundant paths improve fault tolerance at greater cable and interface cost.

Question sources

Data Communication & Networking review questions · Question 5

Question 231 | NS0578

What is the broadcast address of the network 192.168.17.0/24?

A. 192.168.17.0

B. 192.168.17.254

C. 192.168.17.255

D. 192.168.16.255

Hint

Use the cited note definitions to identify the requested function or scope, then check each alternative against that same rule.

Answer C: 192.168.17.255

A /24 prefix fixes the first three octets and leaves eight host bits. Setting them all to one gives final octet 255, so the broadcast is 192.168.17.255. The .0 address is the network boundary and .254 is the last ordinary host; 192.168.16.255 belongs outside the specified /24.

Why each choice is right or wrong

A - Incorrect: 192.168.17.0 has all host bits zero and identifies the network, not broadcast.

B - Incorrect: 192.168.17.254 is the last ordinary host, one below broadcast.

C - Correct: The final eight host bits are all one, giving the /24 broadcast .255.

D - Incorrect: The third octet 16 lies outside network 192.168.17.0/24.

Primary note proof

Study-note section NET24

> Compute network=address AND mask. Host bits zero identify the block start; host bits one give broadcast. With 172.16.28.252/20, the third octet is grouped in blocks of 16, so the network is 172.16.16.0 and broadcast 172.16.31.255. A written host/prefix such as 172.105.180.0/21 need not be an aligned block label: masking yields 172.105.176.0/21.

Study-note section NET25

> For ordinary broadcast LANs let h=32-p. Total addresses=2^h; usable hosts=2^h-2, reserving network and directed broadcast. Find the changing octet's increment as 256-mask octet, round the address down to a multiple, and extend through the next boundary minus one.

Question sources

Data Communication & Networking review questions · Question 6

Question 232 | NS0579

Which device operates at Layer 3 of the OSI model and uses IP addresses to forward data?

A. Hub

B. Bridge

C. Switch

D. Router

Hint

Match the requested scope or data unit to the layer duties in the note; distinguish hop delivery from end-to-end process delivery.

Answer D: Router

IP destination-prefix forwarding between networks is the router function in NET11. Hubs repeat signals and bridges/ordinary switches forward MAC frames at layer 2. Some marketed switches include routing, but the unqualified ordinary switch function in this option set is layer 2; router is the explicit matching device.

Why each choice is right or wrong

A - Incorrect: A hub repeats layer-1 signals rather than forwarding on IP prefixes.

B - Incorrect: A bridge makes layer-2 frame-forwarding decisions using MAC addresses.

C - Incorrect: An ordinary switch is layer 2; a specifically layer-3 switch would require the missing routing qualifier.

D - Correct: Routers inspect destination IP prefixes and choose next hops at layer 3.

Primary note proof

Study-note section NET11

> Routers forward IP packets between networks using destination prefixes and next hops. They separate broadcast domains and normally do not forward local link broadcasts. A default gateway is usually a router, while a protocol gateway can translate application formats; therefore a gateway is not inherently a device that implements every OSI layer.

Study-note section NET10

> A bridge or ordinary Ethernet switch operates at layer 2. It learns source-MAC-to-port mappings, looks up the destination, forwards a known unicast to its port, filters it if the destination is on the incoming segment, and floods an unknown unicast or broadcast within its VLAN. A switch does not always send only to one destination port. Wireless access points normally bridge wireless and wired link-layer traffic.

Study-note section NET09

> A repeater regenerates layer-1 signals without inspecting destination addresses. An active hub is a multiport repeater: it repeats incoming signals onto other ports, placing half-duplex endpoints in one collision domain. A passive hub is a connector. A hub neither learns MAC addresses nor

eliminates collisions. An endpoint such as a network printer consumes services; routers, hubs and access points are intermediary devices.

Question sources

Data Communication & Networking review questions · Question 7

Question 233 | NS0580

UDP is described as a 'connectionless protocol' because it:

A. Cannot transmit video data

B. Does not establish a dedicated connection before sending data and provides no delivery guarantee

C. Only transmits in simplex mode

D. Operates exclusively at the Network Layer

Hint

Identify the requested service or delivery guarantee, then distinguish application roles, transport behavior and address configuration.

Answer B: No setup and no built-in delivery guarantee

UDP's connectionlessness means independent datagrams without built-in setup, not an inability to carry video or an enforced physical duplex mode. It is a transport protocol. B correctly combines no connection establishment with absence of built-in reliable delivery; applications may add their own recovery mechanisms.

Why each choice is right or wrong

A - Incorrect: UDP can carry live media; connectionlessness does not forbid video data.

B - Correct: UDP sends independent datagrams without setup or built-in delivery guarantees.

C - Incorrect: UDP does not impose simplex physical transmission; transport service and physical duplex mode are distinct.

D - Incorrect: UDP is transport-layer, not exclusively a network-layer protocol.

Primary note proof

Study-note section NET17

TCP offers a reliable ordered byte stream using sequence numbers, acknowledgments, retransmission and windows. Flow control protects the receiver; congestion control protects network capacity. UDP sends independent datagrams with ports and a checksum but no built-in setup, delivery guarantee, retransmission or ordering. Live interactive traffic may choose UDP when late data is less useful than lost data. Application protocols can add reliability over UDP.

Study-note section NET06

Simplex is one way, half duplex alternates directions, and full duplex permits simultaneous sending/receiving. A walkie-talkie is half duplex; a telephone conversation uses full duplex. Serial sends sequential bits; parallel uses multiple conductors and may suffer skew. Character-oriented asynchronous serial adds start/stop bits; synchronous framing uses ongoing clock recovery. Neither is synonymous with browser asynchronous requests.

Question sources

Data Communication & Networking review questions · Question 8

Question 234 | NS0581

Assume historical classful addressing and an ordinary broadcast network. A host has address 185.28.17.9. How many usable host addresses are in its default classful network?

A. 254

B. 65,534

C. 16,777,214

D. 65,536

Hint

Convert the mask to a prefix, separate network and host bits, and apply the relevant subnet-count or usable-host rule.

Answer B: 65,534

The first octet 185 lies in the historical Class B range, whose default prefix is /16. That leaves sixteen host bits, yielding 2^16 = 65,536 total addresses. Reserving the network and directed-broadcast addresses gives 65,534 usable hosts. The explicit classful assumption permits deriving the default prefix; modern CIDR would require a stated prefix instead of inferring it from the address.

Why each choice is right or wrong

A - Incorrect: 254 is the usable count for /24, not the Class B default /16.

B - Correct: Class B defaults to /16, giving 2^16−2 = 65,534 usable hosts.

C - Incorrect: 16,777,214 belongs to /8 rather than the Class B default.

D - Incorrect: 65,536 is the /16 total before network and broadcast reservations.

Primary note proof

Study-note section NET22

> Historical classes use leading patterns: A 0 with /8, B 10 with /16, C 110 with /24; D 1110 is multicast and E 1111 reserved. Ordinary class-A first octets are 1-126 because 0 and 127 have special uses. B spans 128-191 and C 192-223. Default usable counts are 2^24-2, 2^16-2 and 254. Modern CIDR requires the actual prefix and overrides class defaults.

Study-note section NET25

> For ordinary broadcast LANs let h=32-p. Total addresses=2^h; usable hosts=2^h-2, reserving network and directed broadcast. Find the changing octet’s increment as 256-mask octet, round the address down to a multiple, and extend through the next boundary minus one.

Question sources

Data Communication & Networking review questions · Question 9

Question 235 | NS0582

Which transmission mode allows simultaneous bidirectional communication?

A. Simplex

B. Half-Duplex

C. Full-Duplex

D. Multipoint

Hint

Use the cited note definitions to identify the requested function or scope, then check each alternative against that same rule.

Answer C: Full duplex

The decisive condition is simultaneous communication in both directions. NET06 defines full duplex exactly that way. Half duplex permits both directions at different times and simplex only one. Multipoint describes sharing a medium among endpoints, not whether two endpoints can send and receive at the same instant.

Why each choice is right or wrong

A - Incorrect: Simplex permits communication in one direction only.

B - Incorrect: Half duplex alternates directions and does not permit simultaneous transmission both ways.

C - Correct: Full duplex supports sending and receiving simultaneously.

D - Incorrect: Multipoint describes medium sharing among endpoints rather than a bidirectional timing mode.

Primary note proof

Study-note section NET06

> Simplex is one way, half duplex alternates directions, and full duplex permits simultaneous sending/receiving. A walkie-talkie is half duplex; a telephone conversation uses full duplex. Serial sends sequential bits; parallel uses multiple conductors and may suffer skew. Character-oriented asynchronous serial adds start/stop bits; synchronous framing uses ongoing clock recovery. Neither is synonymous with browser asynchronous requests.

Study-note section NET08

> Physical topology describes link layout; logical topology describes communication/access relationships. Point-to-point links join two endpoints; multipoint links share a medium. A full mesh consists of point-to-point links.

Question sources

Data Communication & Networking review questions · Question 10

Question 236 | NS0583

The OSI Presentation Layer is primarily responsible for:

A. Routing packets between networks

B. Establishing and ending communication sessions

C. Data compression, encryption, and format translation

D. Physical transmission of raw bits

Hint

Match the requested scope or data unit to the layer duties in the note; distinguish hop delivery from end-to-end process delivery.

Answer C: Compression, encryption and representation translation

NET19 assigns these three representation functions to the OSI presentation layer. Routing belongs to network, dialogs to session and raw bit signaling to physical. Real software can combine roles, but within the stated OSI model C is the specific matching responsibility set.

Why each choice is right or wrong

A - Incorrect: Routing between networks is the network-layer responsibility.

B - Incorrect: Session setup/ending belongs to the session role rather than presentation representation handling.

C - Correct: Compression, encryption and format translation are the presentation roles explicitly listed in NET19.

D - Incorrect: Physical signaling transports bits/symbols rather than translating data representations.

Primary note proof

Study-note section NET19

> OSI session roles establish/manage dialogs and can coordinate checkpoints so transfer resumes after interruption. Presentation roles translate encodings and handle compression/encryption. Compression reduces representation size; encryption hides content and need not shrink it. Application protocols provide services directly to applications. Practical implementations distribute these functions differently; TLS is not proof of a separate physical presentation-layer device.

Study-note section NET30

> Routing computes paths; forwarding chooses a next hop for an individual packet. Select the matching route with the longest prefix, then apply the routing system’s tie-breaking criteria. A default /0 matches when nothing more specific does. Static routes are configured; dynamic protocols exchange reachability. Distance vector uses neighbor estimates, while link state distributes link information and computes shortest paths. Interior protocols operate within an autonomous system; BGP exchanges routes between systems.

Study-note section NET12

Sending proceeds from application data to transport segment/datagram, network packet, link frame and physical bits/symbols; receiving reverses the order. Each layer serves the layer above. A router removes a received link frame, inspects IP, and creates a new link frame for the next hop. MAC addresses usually change across routed hops; end-to-end IP addresses ordinarily remain until translation.

Question sources

Data Communication & Networking review questions · Question 11

Question 237 | NS0584

Which statements are not valid universal guarantees for fiber-optic cable? Select all that apply. Interpret B as a capability with suitable optics and installation, and D as a claim of automatic security.

A. Immunity to electromagnetic interference

B. High bandwidth and long transmission distance

C. Lower initial cost than copper cables

D. High data security due to difficulty of tapping

Hint

Compare the signal mechanism, medium properties or transmission direction against the definitions and stated physical assumptions.

Answer C, D: Lower initial cost than copper cables; High data security due to difficulty of tapping

Fiber guides light, resists electromagnetic interference and can support high capacity over long distances when suitable optics and installation are used. Material alone does not determine a universal installed-cost advantage over copper. Nor does physical tapping difficulty automatically ensure data security: fiber can still be tapped. The selected statements are therefore the unsupported universal guarantees about cost and security, rather than the supported transmission capabilities.

Why each choice is right or wrong

A - Incorrect: EMI resistance follows from light-guided transmission, so this is not a rejected guarantee under the stated scope.

B - Incorrect: With suitable optics and installation, high capacity and long reach are supported capabilities, so this is not selected.

C - Correct: Initial cost depends on optics, reach and installation; lower cost than copper is not universal.

D - Correct: Fiber can be tapped, so automatic high security does not follow from the medium.

Primary note proof

Study-note section NET07

> Twisted pairs reduce coupled interference; UTP has no added shield and STP adds shielding. Coax has an inner conductor and outer shield sharing an axis. Fiber guides light and resists electromagnetic interference; it supports high capacity and long reach, but requires suitable optics and installation. Exact speed, cost and reach depend on the specification, not the material alone. Fiber can still be tapped.

Question sources

Data Communication & Networking review questions · Question 13

Question 238 | NS0585

Which option best defines a dedicated server by its primary workload?

A. A server that also acts as a client

B. A machine whose primary workload is supplying services, even though it may use DNS, backup or update services as a client.

C. A server that handles only file storage

D. Any computer in a peer-to-peer network

Hint

Use the cited note definitions to identify the requested function or scope, then check each alternative against that same rule.

Answer B: A machine whose primary workload is supplying services, even though it may use DNS, backup or update services as a client.

A dedicated server concentrates on supplying services, rather than requiring an absolute prohibition on making any client requests. It may still request DNS resolution, backups or software updates. Merely acting as a client does not define dedication, and dedicated workloads are not limited to file storage. The choice identifies the defining workload while allowing ordinary supporting client activity.

Why each choice is right or wrong

A - Incorrect: A dedicated server may act as a DNS/backup client, but that incidental capability is not its defining dedicated workload.

B - Correct: Concentration on service workloads is the defining dedicated-server characteristic.

C - Incorrect: Dedicated service workloads need not be limited to file storage.

D - Incorrect: An arbitrary peer computer is not thereby a dedicated service-workload server.

Primary note proof

Study-note section NET02

> An intranet serves an organization internally; an extranet exposes selected services to approved outsiders. Neither term alone specifies geographic size. A client requests a service; a server supplies it. Peer systems may perform both roles. Dedicated servers concentrate on service workloads but can still be clients of DNS, backup or update services. A ten-user cutoff is a teaching guideline, not a technical law. Centralization simplifies administration but creates dependencies; peer networks still need security.

Question sources

Data Communication & Networking review questions · Question 14

Question 239 | NS0586

Which protocol operates at the Application Layer of the TCP/IP model and is responsible for translating domain names to IP addresses?

A. SMTP

B. FTP

C. HTTP

D. DNS

Hint

Match the requested scope or data unit to the layer duties in the note; distinguish hop delivery from end-to-end process delivery.

Answer D: DNS

DNS is the name-resolution application protocol in NET20. A/AAAA records provide address data for names. SMTP submits/relays mail, FTP transfers files and HTTP serves web requests; none provides the requested general domain-name record service. Its lookup role is separate from DHCP address assignment.

Why each choice is right or wrong

A - Incorrect: SMTP submits and relays mail rather than resolving hostnames to addresses.

B - Incorrect: FTP transfers files and does not supply the name-resolution record service.

C - Incorrect: HTTP defines web exchanges, not the general hostname-to-address service.

D - Correct: DNS resolves names into records such as A and AAAA address records.

Primary note proof

Study-note section NET20

> DNS resolves names to records, including IPv4 A and IPv6 AAAA addresses; it can use UDP or TCP port 53. DHCP dynamically leases IPv4 settings, commonly address, mask, gateway and DNS server. Its basic exchange is discover, offer, request, acknowledge. IP itself does not assign addresses.

Study-note section NET21

> HTTP defines web request/response semantics; it is stateless, and a message body may be absent. HTTPS adds TLS protection. FTP transfers files using control and separate data connections; it is not the same protocol as SFTP. SMTP submits and relays mail; POP3 retrieves messages and IMAP accesses/synchronizes server mailboxes. Saying SMTP handles both sending and end-user mailbox retrieval is inaccurate.

Question sources

Data Communication & Networking review questions · Question 15

Question 240 | NS0587

Crosstalk is best described as:

A. Loss of signal strength over distance

B. Signals from one communication channel leaking into an adjacent channel

C. Random electron motion causing electrical noise

D. Delay caused by varying signal frequencies

Hint

Compare the signal mechanism, medium properties or transmission direction against the definitions and stated physical assumptions.

Answer B: Leakage from an adjacent communication channel

Crosstalk is unwanted coupling from a neighboring communication channel, directly matching B. Strength loss is attenuation, random thermal motion creates thermal noise and differential frequency delay produces distortion. These impairments can coexist but their definitions are distinct, so the question's mechanism identifies crosstalk specifically.

Why each choice is right or wrong

A - Incorrect: Signal-strength loss is attenuation rather than coupling from a neighboring channel.

B - Correct: Signals leaking into an adjacent channel are crosstalk.

C - Incorrect: Random electron/thermal motion describes thermal noise.

D - Incorrect: Different component-frequency delays distort waveform shape rather than defining crosstalk.

Primary note proof

Study-note section NET06

> Attenuation reduces signal strength. Distortion changes shape, often because frequencies have different delays. Noise adds unwanted energy: thermal noise comes from random thermal motion, crosstalk leaks from nearby channels, and impulse noise is a short disturbance. Amplifiers amplify noise too; digital repeaters regenerate decisions but cannot reconstruct every corrupted bit.

Question sources

Data Communication & Networking review questions · Question 16

Question 241 | NS0588

How many usable host addresses are available in the subnet 192.168.2.64/26?

A. 32

B. 64

C. 62

D. 30

Hint

Convert the mask to a prefix, separate network and host bits, and apply the relevant subnet-count or usable-host rule.

Answer C: 62 usable hosts

A /26 leaves six host bits, so the block has 64 addresses. In the specified block, .64 is the network and .127 the broadcast; usable hosts span .65-.126 inclusive, totaling 62. The question asks usable hosts, not block size, and /31 point-to-point exceptions do not apply.

Why each choice is right or wrong

A - Incorrect: Thirty-two is not the usable count of this /26 block; /26 has 64 total addresses.

B - Incorrect: Sixty-four is the total block size before network/broadcast reservations.

C - Correct: Six host bits give 64 total addresses minus two reservations, leaving 62 usable hosts.

D - Incorrect: Thirty usable hosts is the /27 result, not /26.

Primary note proof

Study-note section NET25

> For ordinary broadcast LANs let h=32-p. Total addresses=2^h; usable hosts=2^h-2, reserving network and directed broadcast. Find the changing octet's increment as 256-mask octet, round the address down to a multiple, and extend through the next boundary minus one.

Study-note section NET25

> 192.168.2.64/26 spans .64-.127; usable .65-.126 gives 62 hosts. 192.168.10.25/28 spans .16-.31, so its network is .16. 172.17.128.0/21 spans 172.17.128.0-172.17.135.255; .128.255 and .135.0 are valid interior hosts, but .135.255 is broadcast. /27 gives 32 total and 30 usable, not 32 usable.

Question sources

Data Communication & Networking review questions · Question 17

Question 242 | NS0589

Which OSI layer is responsible for establishing, maintaining, and ending communication sessions?

A. Transport Layer

B. Session Layer

C. Application Layer

D. Presentation Layer

Hint

Match the requested scope or data unit to the layer duties in the note; distinguish hop delivery from end-to-end process delivery.

Answer B: Session layer

The stem explicitly specifies communication sessions, matching the OSI session role rather than merely a TCP connection. NET19 assigns dialog management and checkpoints to that layer. Transport serves process endpoints, application supplies services and presentation handles representations. B is therefore the specific reference-model lifecycle role.

Why each choice is right or wrong

A - Incorrect: Transport connection state is distinct from the explicitly named OSI session/dialog lifecycle.

B - Correct: Session manages dialogs and their setup, maintenance and recovery/end lifecycle.

C - Incorrect: Application supplies user/application network services rather than the distinct session-layer lifecycle.

D - Incorrect: Presentation translates/compresses/encrypts representations instead of managing dialogs.

Primary note proof

Study-note section NET19

> OSI session roles establish/manage dialogs and can coordinate checkpoints so transfer resumes after interruption. Presentation roles translate encodings and handle compression/encryption. Compression reduces representation size; encryption hides content and need not shrink it. Application protocols provide services directly to applications. Practical implementations distribute these functions differently; TLS is not proof of a separate physical presentation-layer device.

Study-note section NET18

> TCP establishes state with SYN, SYN+ACK, then ACK. SYN consumes one sequence position even with no application bytes. An acknowledgment states the next expected sequence number. For client ISN=395 and server ISN=260: client sends SYN seq395; server sends SYN+ACK seq260 ack396; client sends ACK seq396 ack261. Later byte counts advance sequence numbers. FIN also consumes one sequence position.

Question sources

Data Communication & Networking review questions · Question 18

Question 243 | NS0590

A bus topology network has 20 nodes. If the main cable breaks, what happens?

A. Only the two nodes nearest the break are affected

B. The network continues to function normally

C. The entire network goes down

D. Only the node that caused the break is disconnected

Hint

Draw the links and identify shared components, alternate paths and the effect of the specified failure or growth requirement.

Answer C: A main-backbone break can disrupt the whole basic bus segment

In the conventional single-backbone bus assumed by these options, a main-cable break disrupts the shared segment, affecting the network rather than just one endpoint. NET08 qualifies the physical mechanism as an unterminated break. Redundant segmentation or protected designs are not specified, so C expresses the standard basic-bus failure consequence.

Why each choice is right or wrong

A - Incorrect: A main-backbone fault affects shared signaling, not merely the two closest nodes.

B - Incorrect: A broken unterminated backbone does not preserve normal basic-bus operation.

C - Correct: The shared basic bus segment can fail as a whole when its main backbone is broken.

D - Incorrect: A backbone break differs from an isolated endpoint spur failure and need not be limited to one node.

Primary note proof

Study-note section NET08

> Bus uses a shared backbone; an unterminated break can disrupt the segment. Star connects endpoints through a central device: one edge failure isolates that endpoint, whereas central failure affects the star. Ring forms a loop; basic single rings are vulnerable to a break, while protected dual rings differ. Token passing is associated with Token Ring but is an access method, not a necessary property of every ring. Tree is hierarchical; hybrid combines arrangements.

Question sources

Data Communication & Networking review questions · Question 19

Question 244 | NS0591

Synchronous data transmission differs from asynchronous in that synchronous transmission:

A. Uses start and stop bits for each data chunk

B. Sends data continuously with sender and receiver using the same clock

C. Is always slower than asynchronous

D. Cannot transmit binary data

Hint

Use the cited note definitions to identify the requested function or scope, then check each alternative against that same rule.

Answer B: Ongoing synchronized clock recovery rather than per-character start/stop

NET06 contrasts character start/stop framing with ongoing clock recovery in synchronous transmission. B is the intended synchronized-transfer description; “same clock” should mean synchronized timing, not necessarily a single physical clock device. The note gives no universal speed ordering, and both methods can transmit digital/binary data.

Why each choice is right or wrong

A - Incorrect: Per-character start/stop bits describe character-oriented asynchronous serial transmission.

B - Correct: Synchronous transfer maintains coordinated timing through ongoing clock recovery rather than character start/stop framing.

C - Incorrect: No universal slower-than-asynchronous rule follows from the timing method.

D - Incorrect: Synchronous framing can carry binary data; the timing convention does not prohibit it.

Primary note proof

Study-note section NET06

> Simplex is one way, half duplex alternates directions, and full duplex permits simultaneous sending/receiving. A walkie-talkie is half duplex; a telephone conversation uses full duplex. Serial sends sequential bits; parallel uses multiple conductors and may suffer skew. Character-oriented asynchronous serial adds start/stop bits; synchronous framing uses ongoing clock recovery. Neither is synonymous with browser asynchronous requests.

Question sources

Data Communication & Networking review questions · Question 20

Question 245 | NS0592

What is the PRIMARY function of the Network Layer (Layer 3)?

A. Providing physical transmission of bits

B. Error detection and MAC addressing

C. End-to-end routing of data between different networks using IP addresses

D. Establishing communication sessions between applications

Hint

Match the requested scope or data unit to the layer duties in the note; distinguish hop delivery from end-to-end process delivery.

Answer C: Logical IP addressing and routing across networks

NET12 gives network-layer logical addressing and routing; NET11 explains forwarding IP packets among networks by destination prefixes. C directly states that responsibility. The other options assign physical signaling, link MAC/error detection and session-dialog management, which belong to different model layers.

Why each choice is right or wrong

A - Incorrect: Transporting raw physical bits/symbols is the physical-layer function.

B - Incorrect: MAC addressing and hop frame error detection are data-link responsibilities.

C - Correct: Network-layer logical addressing and routing carry IP packets between networks.

D - Incorrect: Establishing application dialogs is a session-layer role rather than IP routing.

Primary note proof

Study-note section NET11

> Routers forward IP packets between networks using destination prefixes and next hops. They separate broadcast domains and normally do not forward local link broadcasts. A default gateway is usually a router, while a protocol gateway can translate application formats; therefore a gateway is not inherently a device that implements every OSI layer.

Study-note section NET12

> Sending proceeds from application data to transport segment/datagram, network packet, link frame and physical bits/symbols; receiving reverses the order. Each layer serves the layer above. A router removes a received link frame, inspects IP, and creates a new link frame for the next hop. MAC addresses usually change across routed hops; end-to-end IP addresses ordinarily remain until translation.

Study-note section NET19

> OSI session roles establish/manage dialogs and can coordinate checkpoints so transfer resumes after interruption. Presentation roles translate encodings and handle compression/encryption. Compression reduces representation size; encryption hides content and need not shrink it. Application protocols provide services directly to applications. Practical implementations

distribute these functions differently; TLS is not proof of a separate physical presentation-layer device.

Question sources

Data Communication & Networking review questions · Question 21

Question 246 | NS0593

Which of the following IPv4 addresses is INVALID?

A. 192.168.0.1

B. 10.0.0.255

C. 172.16.254.1

D. 10.256.0.1

Hint

Separate address width, syntax, reserved scope and the supplied prefix or historical classful convention.

Answer D: 10.256.0.1 has an impossible octet

An IPv4 decimal octet must fit eight bits, from 0 through 255. D has 256 and is therefore syntactically invalid. A-C each meet that range condition. B's .255 ending alone does not establish a broadcast without a prefix, so it cannot be rejected merely by its last octet.

Why each choice is right or wrong

A - Incorrect: All four octets are within 0-255, so this notation is valid.

B - Incorrect: Every octet is valid; a .255 ending alone does not determine broadcast status without a prefix.

C - Incorrect: All four values fit eight-bit octets and form valid dotted-decimal notation.

D - Correct: The second octet 256 exceeds the maximum representable eight-bit value 255.

Primary note proof

Study-note section NET22

Write IPv4 as four decimal octets 0-255, or as 32 binary bits. Use weights 128,64,32,16,8,4,2,1 within each octet. Thus 11000001 10000011 00011011 11111111 is 193.131.27.255. A value such as 257 is impossible. Syntactic validity differs from assignability: an address ending .0 or .255 can be a host under some prefixes.

Question sources

Data Communication & Networking review questions · Question 22

Question 247 | NS0594

In IPv6, addresses are how many bits long?

A. 32 bits

B. 64 bits

C. 96 bits

D. 128 bits

Hint

Separate address width, syntax, reserved scope and the supplied prefix or historical classful convention.

Answer D: 128 bits

NET23 explicitly gives IPv6 addresses a 128-bit width. IPv4 uses 32 bits; 64 may describe a common subnet interface boundary but is not the whole IPv6 address length. Ninety-six bits is likewise not the full width. D therefore answers the requested address size.

Why each choice is right or wrong

A - Incorrect: Thirty-two bits is the IPv4 address width, not IPv6.

B - Incorrect: Sixty-four bits is not the complete IPv6 address width.

C - Incorrect: Ninety-six bits does not match the specified 128-bit IPv6 address length.

D - Correct: IPv6 addresses contain 128 bits as explicitly stated in NET23.

Primary note proof

Study-note section NET23

> IPv6 has 128-bit hexadecimal addresses, flexible prefixes and no IPv4-style broadcast. Sources, not routers, fragment IPv6 packets. IPv6 does not automatically encrypt traffic or make authentication unnecessary. Compare IPv6's larger 128-bit address space and encryption support separately; specify the property being evaluated.

Study-note section NET16

> IP supplies connectionless best-effort packet delivery, not end-to-end ordering or retransmission. IPv4 addresses are 32 bits. Its minimum header is 20 bytes and can grow to 60 bytes; it is not a 32-bit header. IHL counts 32-bit words; total length includes header and payload. TTL limits lifetime across routers; the protocol field identifies TCP, UDP or another upper-layer protocol.

Study-note section NET-S06

> A common IPv6 unicast subnet uses a 64-bit subnet prefix and a 64-bit interface identifier. This split does not make the complete address 64 bits: it remains 128 bits. Special uses and explicitly different prefix lengths must be considered separately.

Question sources

Data Communication & Networking review questions · Question 23

Question 248 | NS0595

A bridge decides whether to forward a frame to another network segment by examining the:

A. IP address in the packet header

B. Port number in the segment header

C. Source and destination MAC addresses

D. TTL (Time to Live) field

Hint

Compare signal repetition, frame forwarding, packet routing and policy enforcement using the stated device or traffic assumptions.

Answer C: Learn source MACs and forward according to destination MAC

A bridge learns which sources are reachable through each port and consults the destination MAC when forwarding/filtering a frame. C names the relevant link addresses. IP, transport ports and TTL belong to higher-layer packet/segment processing, not the ordinary bridge forwarding decision. Unknown destinations may be flooded, so learning does not imply always-one-port forwarding.

Why each choice is right or wrong

A - Incorrect: Destination IP prefixes drive routing, not ordinary layer-2 bridge frame forwarding.

B - Incorrect: Transport ports identify process endpoints and are not the bridge MAC-table lookup key.

C - Correct: Source MAC informs learning and destination MAC informs forwarding/filtering to the appropriate segment.

D - Incorrect: TTL is an IP header field used in routed packet lifetime, not ordinary bridging.

Primary note proof

Study-note section NET10

> A bridge or ordinary Ethernet switch operates at layer 2. It learns source-MAC-to-port mappings, looks up the destination, forwards a known unicast to its port, filters it if the destination is on the incoming segment, and floods an unknown unicast or broadcast within its VLAN. A switch does not always send only to one destination port. Wireless access points normally bridge wireless and wired link-layer traffic.

Study-note section NET17

> Ports identify transport endpoints; the application can choose a transport and request socket buffer sizes, subject to OS limits. A TCP connection is identified by source/destination IP and source/destination port, with TCP understood. IPv4 protocol numbers identify upper protocols; 80 is a usual HTTP port, not an IP protocol number. Clients often use ephemeral ports. SCTP is a reliable message-oriented transport with multiple streams.

Study-note section NET16

IP supplies connectionless best-effort packet delivery, not end-to-end ordering or retransmission. IPv4 addresses are 32 bits. Its minimum header is 20 bytes and can grow to 60 bytes; it is not a 32-bit header. IHL counts 32-bit words; total length includes header and payload. TTL limits lifetime across routers; the protocol field identifies TCP, UDP or another upper-layer protocol.

Question sources

Data Communication & Networking review questions · Question 24

Question 249 | NS0596

Circuit switching guarantees bandwidth for the duration of a call. What is the main DISADVANTAGE of this?

A. High latency during transmission

B. Bandwidth is wasted when no data is actively being transmitted

C. Packets may arrive out of order

D. It cannot support voice communication

Hint

Compare signal repetition, frame forwarding, packet routing and policy enforcement using the stated device or traffic assumptions.

Answer B: Reserved bandwidth can be wasted during silence

Circuit switching holds resources for the call even while endpoints are silent, so unused reservation cannot be statistically shared as packet traffic would be. B gives that cost. Circuit switching does not inherently deliver packets out of order or prevent voice transmission; traditional telephone calls are a standard example.

Why each choice is right or wrong

A - Incorrect: Reserved circuits can offer predictable transfer behavior; setup cost is distinct from universally high transfer latency.

B - Correct: Capacity remains reserved during silence and can be wasted when no data is sent.

C - Incorrect: Independent out-of-order packet routing is not the defining reserved-circuit disadvantage.

D - Incorrect: Traditional telephone calls are the note's standard circuit-switching example, so voice is supported.

Primary note proof

Study-note section NET31

> Circuit switching sets up a path with reserved resources, transfers data, then releases it. Predictable allocated bandwidth trades against setup/blocking and wasted reservation during silence. A traditional telephone call is the standard example. Packet switching divides data into packets that share links statistically; queueing can add variable delay and loss. This does not make modern voice-over-packet impossible: buffering, scheduling and capacity planning manage it.

Question sources

Data Communication & Networking review questions · Question 25

Question 250 | NS0597

Under the textbook direct line-of-sight wireless-link convention, which option gives the most complete set of listed technologies whose direct path can be blocked by buildings or terrain? Treat radio waves as the broad category rather than assuming every radio propagation mode needs line of sight.

A. Radio waves

B. Microwaves

C. Infrared

D. Both B and C

Hint

Compare the signal mechanism, medium properties or transmission direction against the definitions and stated physical assumptions.

Answer D: Microwave and infrared under the conventional line-of-sight assumption

Conventional directional microwave links need suitable path visibility, and infrared generally does not penetrate walls. Obstacles can therefore interrupt the direct links specified here. Both individual technologies fit, so the combined option is the complete response. Radio waves is a broader physical category that includes microwave but also other propagation modes; the question does not assert that all radio links share the same line-of-sight restriction.

Why each choice is right or wrong

A - Incorrect: The broad radio category includes propagation modes beyond the specified line-of-sight comparison.

B - Incorrect: Microwave fits the stated direct-link case, but this alone omits infrared.

C - Incorrect: Infrared fits the stated obstructed-direct-path case, but this alone omits microwave.

D - Correct: Both microwave and infrared fit the specified comparison, making this the complete set.

Primary note proof

Study-note section NET07

> Radio, microwave and infrared are unguided media. Ground waves follow Earth, sky waves can reflect from ionized layers, and line-of-sight paths require suitable visibility. Microwaves are radio waves in the broader physical classification. Infrared generally does not penetrate walls. Directionality depends on antennas: omnidirectional means broad azimuth coverage, not equal radiation in every 3-D direction. Legacy Ethernet straight-through cables join unlike MDI/MDI-X roles; crossover joins like roles, such as PC-PC or switch-switch. Auto-MDI-X can remove that requirement.

Question sources

Data Communication & Networking review questions · Question 26

Question 251 | NS0598

What does CIDR stand for, and what problem did it solve?

A. Classless Inter-Domain Routing; it solved address wastage in classful addressing

B. Classful Internet Domain Routing; it solved packet loss

C. Centralized IP Domain Routing; it solved routing loops

D. Classless Internet Data Routing; it solved latency in WANs

Hint

Apply the cited definitions to the stated scope; for calculations, derive the result from the supplied prefix, bit count or resource rule.

Answer A: Classless Inter-Domain Routing; flexible prefixes reduce rigid class allocation waste

CIDR replaces rigid class allocation. Flexible prefixes allow blocks sized to requirements and aggregation of aligned blocks, addressing waste from fixed historical class sizes. The other expansions are incorrect and their proposed packet-loss, loop or latency cures are not the defined purpose.

Why each choice is right or wrong

A - Correct: This gives the correct expansion and relates flexible prefix allocation to avoiding rigid class-size waste.

B - Incorrect: Classful Internet Domain Routing is the wrong expansion, and CIDR is not defined as a packet-loss cure.

C - Incorrect: Centralized IP Domain Routing is not the acronym expansion or the stated mechanism.

D - Incorrect: Classless Internet Data Routing is incorrect; CIDR is not defined as a general WAN-latency cure.

Primary note proof

Study-note section NET28

> CIDR, Classless Inter-Domain Routing, replaces rigid class allocation and supports aggregation. Combine contiguous aligned blocks sharing leading bits; unrelated adjacent-looking labels may not aggregate cleanly. Four consecutive /26 blocks covering a /24 summarize to /24. More-specific routes must remain available where the aggregate would otherwise send traffic to the wrong next hop.

Study-note section NET26

> For H hosts, choose the smallest h satisfying 2^h-2≥H, then p=32-h. For 24 hosts use /27; 52 or 57 use /26; 100 use /25; 500 use /23. For at least six equal subnets choose b=3. A Class C /24 split to /27 yields eight subnets. Always check both the number of subnets and the host capacity.

Question sources

Data Communication & Networking review questions · Question 27

Question 252 | NS0599

How many subnets are created when you borrow 5 bits from the host portion of a Class B network?

A. 5

B. 16

C. 32

D. 64

Hint

Apply the cited definitions to the stated scope; for calculations, derive the result from the supplied prefix, bit count or resource rule.

Answer C: 32 subnets

Borrowing five bits yields 2^5=32 equal subnets under modern counting. The parent Class B /16 would become /21, but the direct subnet count only needs the specified five borrowed bits. NET26 says not to subtract two subnets under modern practice.

Why each choice is right or wrong

A - Incorrect: Five is the number of borrowed bits, not the exponential number of resulting subnet combinations.

B - Incorrect: Sixteen subnets would use four borrowed bits rather than five.

C - Correct: Five borrowed bits have 32 distinct combinations and therefore produce 32 subnets.

D - Incorrect: Sixty-four subnets would require six borrowed bits.

Primary note proof

Study-note section NET26

> To split parent /a into equal /p blocks, borrow b=p-a bits and obtain 2^b subnets. Do not subtract two subnets under modern practice. For a Class B /16 parent split to /19, b=3 gives eight subnets, each with 8192 addresses and 8190 conventional hosts. A /19 alone does not state its parent.

Question sources

Data Communication & Networking review questions · Question 28

Question 253 | NS0600

The 'forwarding table' in a bridge is also known as the:

A. Routing table

B. ARP table

C. MAC table

D. IP table

Hint

Apply the cited definitions to the stated scope; for calculations, derive the result from the supplied prefix, bit count or resource rule.

Answer C: MAC table

The bridge forwarding database records MAC-to-port associations learned from source addresses and used for destination lookups. MAC table is therefore the matching name. A routing table maps IP prefixes to next hops; ARP associates on-link IPv4 addresses with link addresses. Those are different tables even if one device maintains several of them.

Why each choice is right or wrong

A - Incorrect: Routing tables describe destination IP prefixes and next hops rather than bridge MAC-to-port mappings.

B - Incorrect: ARP caches associate IPv4 next hops with link addresses, not MAC addresses with bridge ports.

C - Correct: The bridge's learned source-MAC-to-port forwarding database is its MAC table.

D - Incorrect: IP table does not name the layer-2 learned MAC forwarding database described in NET10.

Primary note proof

Study-note section NET-S06

> A bridge or switch's MAC address table is its learned forwarding database: it associates MAC addresses with ports for frame forwarding. It differs from an ARP cache, which associates an IPv4 next hop with a link address, and from a routing table, which selects next hops for IP prefixes.

Study-note section NET10

> A bridge or ordinary Ethernet switch operates at layer 2. It learns source-MAC-to-port mappings, looks up the destination, forwards a known unicast to its port, filters it if the destination is on the incoming segment, and floods an unknown unicast or broadcast within its VLAN. A switch does not always send only to one destination port. Wireless access points normally bridge wireless and wired link-layer traffic.

Question sources

Data Communication & Networking review questions · Question 29

Question 254 | NS0601

Which layer of the OSI model is responsible for defining voltage levels, cable specifications, and how bits are physically transmitted?

A. Data Link Layer

B. Network Layer

C. Physical Layer

D. Transport Layer

Hint

Apply the cited definitions to the stated scope; for calculations, derive the result from the supplied prefix, bit count or resource rule.

Answer C: Physical layer

Voltage, cable/interface characteristics and signal transport are the physical-layer scope in NET09. Data-link functions operate on frames and MAC access, network handles IP routing and transport handles process delivery. The wording explicitly asks how bits are physically represented and carried, so C is the corresponding layer.

Why each choice is right or wrong

A - Incorrect: Data link manages frames/access rather than defining the physical voltage and cable interface.

B - Incorrect: Network manages logical addressing/routing rather than electrical signal specifications.

C - Correct: Physical-layer specifications include connectors, signaling, voltage and timing.

D - Incorrect: Transport supplies process delivery rather than cable and voltage definitions.

Primary note proof

Study-note section NET09

> A NIC supplies a computer’s network interface and commonly implements both physical and link functions. Calling a NIC a physical interface does not mean all its functions are layer 1. Physical specifications include connectors, signaling, voltage, timing and physical coding/modulation; the PHY interface to MAC handles hardware signaling.

Study-note section NET12

> Sending proceeds from application data to transport segment/datagram, network packet, link frame and physical bits/symbols; receiving reverses the order. Each layer serves the layer above. A router removes a received link frame, inspects IP, and creates a new link frame for the next hop. MAC addresses usually change across routed hops; end-to-end IP addresses ordinarily remain until translation.

Question sources

Data Communication & Networking review questions · Question 30

Question 255 | NS0602

In a star topology, what happens if the central hub fails?

A. Only the hub's nearest neighbor is affected

B. The entire network fails

C. The network continues operating in bus mode

D. Nodes automatically reconnect in ring topology

Hint

Apply the cited definitions to the stated scope; for calculations, derive the result from the supplied prefix, bit count or resource rule.

Answer B: The dependent star loses connectivity when its center fails

In a basic star every endpoint depends on the central hub for communication with other endpoints. Failure of that common center therefore affects the whole star. No alternate center or automatic topology reconfiguration is specified; the network does not become a bus or ring merely because the hub stops functioning.

Why each choice is right or wrong

A - Incorrect: The center serves all star endpoints, so its failure is not limited to the nearest neighbor.

B - Correct: All endpoints depend on the central hub, so the basic star loses inter-endpoint connectivity.

C - Incorrect: A hub failure does not physically or logically rewire the star into an operational bus.

D - Incorrect: No automatic ring reconnection mechanism follows from the basic star topology.

Primary note proof

Study-note section NET08

> Bus uses a shared backbone; an unterminated break can disrupt the segment. Star connects endpoints through a central device: one edge failure isolates that endpoint, whereas central failure affects the star. Ring forms a loop; basic single rings are vulnerable to a break, while protected dual rings differ. Token passing is associated with Token Ring but is an access method, not a necessary property of every ring. Tree is hierarchical; hybrid combines arrangements.

Question sources

Data Communication & Networking review questions · Question 31

Question 256 | NS0603

What type of noise CANNOT be completely eliminated because it is caused by the random motion of electrons due to temperature?

A. Crosstalk

B. Impulse noise

C. Thermal noise

D. Intermodulation noise

Hint

Apply the cited definitions to the stated scope; for calculations, derive the result from the supplied prefix, bit count or resource rule.

Answer C: Thermal noise

The stated cause-random motion associated with temperature-is thermal noise in NET06. Crosstalk is neighboring-channel coupling and impulse noise is a short disturbance. D names a different noise phenomenon not defined by random thermal motion. The cause identifies C without requiring a claim that all other real noise can be perfectly eliminated.

Why each choice is right or wrong

A - Incorrect: Crosstalk arises from coupling between nearby communication channels, not the stated thermal-motion cause.

B - Incorrect: Impulse noise is a short disturbance rather than persistent random thermal motion.

C - Correct: Thermal noise is explicitly caused by random thermal motion, matching the temperature-dependent clue.

D - Incorrect: This option does not match the random thermal-motion definition supplied in NET06.

Primary note proof

Study-note section NET06

> Attenuation reduces signal strength. Distortion changes shape, often because frequencies have different delays. Noise adds unwanted energy: thermal noise comes from random thermal motion, crosstalk leaks from nearby channels, and impulse noise is a short disturbance. Amplifiers amplify noise too; digital repeaters regenerate decisions but cannot reconstruct every corrupted bit.

Study-note section NET-S07

> Intermodulation distortion occurs when multiple signals interact through a nonlinear component and generate unwanted combination-frequency products. Its mechanism differs from random thermal motion, adjacent-channel leakage and an isolated impulse disturbance.

Question sources

Data Communication & Networking review questions · Question 32

Question 257 | NS0604

Which IP address class has a first-octet range of 128-191?

A. Class A

B. Class B

C. Class C

D. Class D

Hint

Apply the cited definitions to the stated scope; for calculations, derive the result from the supplied prefix, bit count or resource rule.

Answer B: Class B

NET22 gives first-octet 128-191 for historical Class B, corresponding to leading bits 10. Ordinary Class A is 1-126, Class C is 192-223 and Class D uses leading 1110 for multicast. Since the question explicitly asks classes, the historical categorization is appropriate rather than inferring a current CIDR prefix.

Why each choice is right or wrong

A - Incorrect: Ordinary historical Class A uses first octets 1-126 rather than 128-191.

B - Correct: Historical Class B spans first octets 128-191, with leading bits 10.

C - Incorrect: Historical Class C spans 192-223, above the supplied interval.

D - Incorrect: Class D multicast begins with 1110, outside the Class B 128-191 interval.

Primary note proof

Study-note section NET22

> Historical classes use leading patterns: A 0 with /8, B 10 with /16, C 110 with /24; D 1110 is multicast and E 1111 reserved. Ordinary class-A first octets are 1-126 because 0 and 127 have special uses. B spans 128-191 and C 192-223. Default usable counts are 2^24-2, 2^16-2 and 254. Modern CIDR requires the actual prefix and overrides class defaults.

Question sources

Data Communication & Networking review questions · Question 33

Question 258 | NS0605

The Session Layer's 'checkpointing' feature means that it:

A. Encrypts data to protect it from interception

B. Compresses data to reduce transmission time

C. Saves the state of a communication session at regular intervals so it can be resumed after interruption

D. Translates data between different character encoding formats

Hint

Apply the cited definitions to the stated scope; for calculations, derive the result from the supplied prefix, bit count or resource rule.

Answer C: Checkpoint state supports resuming after interruption

A checkpoint records recoverable progress/state so interrupted work can resume from an agreed point. NET19 assigns such coordination to the session role. Encryption, compression and encoding translation belong to representation handling and do not by themselves preserve resumable dialog progress. C matches the checkpoint recovery purpose.

Why each choice is right or wrong

A - Incorrect: Encryption conceals content and does not define saving resumable session progress.

B - Incorrect: Compression reduces representation size rather than recording recovery checkpoints.

C - Correct: Saving agreed progress/state enables continuation after interruption rather than restarting from the beginning.

D - Incorrect: Encoding translation changes representation format, not checkpoint recovery state.

Primary note proof

Study-note section NET19

> OSI session roles establish/manage dialogs and can coordinate checkpoints so transfer resumes after interruption. Presentation roles translate encodings and handle compression/encryption. Compression reduces representation size; encryption hides content and need not shrink it. Application protocols provide services directly to applications. Practical implementations distribute these functions differently; TLS is not proof of a separate physical presentation-layer device.

Question sources

Data Communication & Networking review questions · Question 34

Question 259 | NS0606

Which of the following is a De Jure standard?

A. A manufacturer's proprietary cable format adopted industry-wide

B. A standard officially approved by ISO or IEEE

C. A standard developed by a single corporation without regulatory approval

D. A protocol widely used but never formally documented

Hint

Apply the cited definitions to the stated scope; for calculations, derive the result from the supplied prefix, bit count or resource rule.

Answer B: A formally approved standard

NET03 defines de jure by formal approval. B directly states official approval, while industry adoption without that approval is de facto. Corporate origin does not alone decide status, but C specifically lacks formal approval and D emphasizes informal use. Therefore B is the option establishing the defining approval condition.

Why each choice is right or wrong

A - Incorrect: Widespread adoption alone demonstrates de facto use rather than formal de jure approval.

B - Correct: Official approval matches the defining de jure criterion in NET03.

C - Incorrect: A corporate format without the stated formal approval does not meet the offered de jure definition.

D - Incorrect: Widespread informal use without formal approval is de facto rather than de jure.

Primary note proof

Study-note section NET03

> Protocol syntax defines message structure, semantics defines field meanings, and timing defines when/how fast exchanges occur. A standard supports interoperability. De facto means established through use; de jure means formally approved. ISO develops international standards; IEEE develops LAN standards such as 802.3 and 802.11; ITU-T develops telecommunications standards. ANSI coordinates US standards, EIA is associated with interface standards, and FCC is a regulator.

Question sources

Data Communication & Networking review questions · Question 35

Question 260 | NS0607

Parallel data transmission sends multiple bits simultaneously. Its key DISADVANTAGE compared to serial transmission is:

A. It is always slower

B. It cannot be used for digital data

C. It requires more transmission lines and can suffer from interference between lines

D. It only works over fiber-optic cable

Hint

Apply the cited definitions to the stated scope; for calculations, derive the result from the supplied prefix, bit count or resource rule.

Answer C: More conductors and interline impairments

Parallel transfer needs several conductors to carry simultaneous bits. Those paths can experience skew and neighboring-channel coupling, as NET06's impairment definitions explain. C states the extra-line and interference burden. No universal slower-speed claim, inability to carry digital data or fiber-only restriction follows from parallel transmission.

Why each choice is right or wrong

A - Incorrect: Parallel is not universally slower; performance depends on implementation, distance and synchronization.

B - Incorrect: Parallel transmission can carry digital bits simultaneously, exactly as the stem states.

C - Correct: Multiple conductors add wiring and can suffer skew or coupled interference between adjacent lines.

D - Incorrect: Parallel transmission is not restricted to fiber and commonly concerns multiple electrical conductors.

Primary note proof

Study-note section NET06

> Simplex is one way, half duplex alternates directions, and full duplex permits simultaneous sending/receiving. A walkie-talkie is half duplex; a telephone conversation uses full duplex. Serial sends sequential bits; parallel uses multiple conductors and may suffer skew. Character-oriented asynchronous serial adds start/stop bits; synchronous framing uses ongoing clock recovery. Neither is synonymous with browser asynchronous requests.

Study-note section NET06

> Attenuation reduces signal strength. Distortion changes shape, often because frequencies have different delays. Noise adds unwanted energy: thermal noise comes from random thermal motion, crosstalk leaks from nearby channels, and impulse noise is a short disturbance. Amplifiers amplify noise too; digital repeaters regenerate decisions but cannot reconstruct every corrupted bit.

Question sources

Data Communication & Networking review questions · Question 36

Question 261 | NS0608

A packet-switching network may be UNSUITABLE for real-time voice communication because:

A. It requires a dedicated circuit

B. Variable latency and possible packet loss can disrupt real-time audio

C. It cannot carry voice signals

D. All bandwidth is reserved, leaving none for voice

Hint

Apply the cited definitions to the stated scope; for calculations, derive the result from the supplied prefix, bit count or resource rule.

Answer B: Variable delay and packet loss can disturb real-time audio

Real-time audio is sensitive to late or missing data. Packet networks may introduce variable queueing delay and loss, so B gives a plausible suitability issue. Modern voice over packets remains possible with buffering, scheduling and capacity planning; it is not intrinsically prohibited or dependent on reserved circuits.

Why each choice is right or wrong

A - Incorrect: Datagram packet switching does not require a dedicated circuit before every communication.

B - Correct: Variable queueing latency and loss can make audio arrive late or incomplete.

C - Incorrect: NET31 explicitly allows voice over packets with suitable engineering.

D - Incorrect: Statistical link sharing differs from reserving all bandwidth for established circuits.

Primary note proof

Study-note section NET31

> Circuit switching sets up a path with reserved resources, transfers data, then releases it. Predictable allocated bandwidth trades against setup/blocking and wasted reservation during silence. A traditional telephone call is the standard example. Packet switching divides data into packets that share links statistically; queueing can add variable delay and loss. This does not make modern voice-over-packet impossible: buffering, scheduling and capacity planning manage it.

Study-note section NET17

> TCP offers a reliable ordered byte stream using sequence numbers, acknowledgments, retransmission and windows. Flow control protects the receiver; congestion control protects network capacity. UDP sends independent datagrams with ports and a checksum but no built-in

setup, delivery guarantee, retransmission or ordering. Live interactive traffic may choose UDP when late data is less useful than lost data. Application protocols can add reliability over UDP.

Question sources

Data Communication & Networking review questions · Question 37

Question 262 | NS0609

For a Class C network subnetted to /27, how many usable hosts per subnet are available?

A. 32

B. 30

C. 28

D. 62

Hint

Apply the cited definitions to the stated scope; for calculations, derive the result from the supplied prefix, bit count or resource rule.

Answer B: 30 usable hosts

A /27 leaves five host bits regardless of the historical class of its parent. Those bits provide 32 total addresses. On an ordinary broadcast subnet, network and broadcast reserve two, leaving 30 usable host addresses. Parent classification matters for subnet counting, not this explicit-prefix host calculation.

Why each choice is right or wrong

A - Incorrect: Thirty-two is the total address count before reserving network and broadcast.

B - Correct: Five host bits give 32−2=30 ordinary usable hosts.

C - Incorrect: Twenty-eight does not follow from the stated five host bits and two standard reservations.

D - Incorrect: Sixty-two usable hosts corresponds to /26 rather than the supplied /27.

Primary note proof

Study-note section NET25

For ordinary broadcast LANs let h=32-p. Total addresses=2^h; usable hosts=2^h-2, reserving network and directed broadcast. Find the changing octet’s increment as 256-mask octet, round the address down to a multiple, and extend through the next boundary minus one.

Question sources

Data Communication & Networking review questions · Question 38

Question 263 | NS0610

Which routing type sends data to the NEAREST of multiple hosts sharing the same IP address?

A. Multicast

B. Broadcast

C. Unicast

D. Anycast

Hint

Apply the cited definitions to the stated scope; for calculations, derive the result from the supplied prefix, bit count or resource rule.

Answer D: Anycast

Anycast routes to one member of a set sharing the address, typically the nearest by routing metrics. That is not necessarily geographic distance. Multicast targets a subscribed group, broadcast all in scope and ordinary unicast a single designated destination. D uniquely matches the shared-address nearest-member rule.

Why each choice is right or wrong

A - Incorrect: Multicast targets a subscribed group rather than selecting only one nearest shared-address member.

B - Incorrect: Broadcast targets all destinations within its scope, not the nearest member.

C - Incorrect: Ordinary unicast targets one designated destination without the shared-address nearest-member semantics.

D - Correct: Anycast selects one shared-address member, normally nearest according to routing metrics.

Primary note proof

Study-note section NET30

> Flooding sends copies on eligible outgoing links with duplicate/lifetime controls; random walk picks a neighbor probabilistically. Unicast targets one destination, broadcast all in a scope, multicast a subscribed group and anycast one member sharing an address, normally nearest under routing metrics. Multi-destination packets can list multiple targets; this is not necessarily identical to broadcast. Group multicast trees use mechanisms such as reverse-path checks; Ethernet spanning tree is a different layer-2 mechanism.

Question sources

Data Communication & Networking review questions · Question 39

Question 264 | NS0611

The term 'coaxial' refers to the fact that the cable's inner conductor and outer shield:

A. Are made of the same conductive material

B. Share the same central axis

C. Carry signals in opposite directions

D. Are both covered in plastic insulation

Hint

Apply the cited definitions to the stated scope; for calculations, derive the result from the supplied prefix, bit count or resource rule.

Answer B: The conductor and shield share an axis

The name coaxial refers to a common geometric axis for the inner conductor and surrounding shield. NET07 states this directly. Neither identical material, opposite signal directions nor a particular insulation covering defines the term; those are separate construction or usage details rather than the shared-axis relationship.

Why each choice is right or wrong

A - Incorrect: The definition concerns geometric arrangement, not whether both conductive parts use the same material.

B - Correct: The inner conductor and outer shield share a central axis, giving the coaxial name.

C - Incorrect: Opposite signal directions are not the defining common-axis geometry.

D - Incorrect: Insulation details do not define coaxial; sharing an axis does.

Primary note proof

Study-note section NET07

> Twisted pairs reduce coupled interference; UTP has no added shield and STP adds shielding. Coax has an inner conductor and outer shield sharing an axis. Fiber guides light and resists electromagnetic interference; it supports high capacity and long reach, but requires suitable optics and installation. Exact speed, cost and reach depend on the specification, not the material alone. Fiber can still be tapped.

Question sources

Data Communication & Networking review questions · Question 40

Question 265 | NS0612

Which option best describes a protocol-translating gateway joining unlike networked systems?

A. A device that boosts signal strength over long distances

B. A device that connects networks using the same protocol

C. A device that connects two or more networks using different protocols, topologies, or architectures

D. A device that filters traffic based on MAC addresses

Hint

Apply the cited definitions to the stated scope; for calculations, derive the result from the supplied prefix, bit count or resource rule.

Answer C: A device that connects two or more networks using different protocols, topologies, or architectures

Gateway has several networking meanings. A default IP gateway is commonly a router, while a protocol gateway translates between unlike protocols or application formats. The question asks for that translating role, so the option joining unlike systems fits. Signal regeneration belongs to repeaters, same-protocol routing does not require translation, and MAC-based filtering describes bridging or switching rather than protocol conversion.

Why each choice is right or wrong

A - Incorrect: Signal regeneration/strength extension is a repeater function rather than either gateway meaning defined here.

B - Incorrect: Connecting networks using the same protocol describes routing without the required protocol translation.

C - Correct: A protocol gateway joins unlike systems through the translation required by the stated scope.

D - Incorrect: MAC-address frame filtering describes bridging/switching rather than the gateway distinction in NET11.

Primary note proof

Study-note section NET11

> Routers forward IP packets between networks using destination prefixes and next hops. They separate broadcast domains and normally do not forward local link broadcasts. A default gateway is usually a router, while a protocol gateway can translate application formats; therefore a gateway is not inherently a device that implements every OSI layer.

Study-note section NET10

> A bridge or ordinary Ethernet switch operates at layer 2. It learns source-MAC-to-port mappings, looks up the destination, forwards a known unicast to its port, filters it if the destination is on the incoming segment, and floods an unknown unicast or broadcast within its VLAN. A switch does

not always send only to one destination port. Wireless access points normally bridge wireless and wired link-layer traffic.

Study-note section NET09

A repeater regenerates layer-1 signals without inspecting destination addresses. An active hub is a multiport repeater: it repeats incoming signals onto other ports, placing half-duplex endpoints in one collision domain. A passive hub is a connector. A hub neither learns MAC addresses nor eliminates collisions. An endpoint such as a network printer consumes services; routers, hubs and access points are intermediary devices.

Question sources

Data Communication & Networking review questions · Question 41

Question 266 | NS0613

An organization is assigned the Class A IP address 10.200.240.4. What is the network address?

A. 10.0.0.0

B. 10.200.0.0

C. 10.200.240.0

D. 0.0.0.0

Hint

Apply the cited definitions to the stated scope; for calculations, derive the result from the supplied prefix, bit count or resource rule.

Answer A: 10.0.0.0 under the explicitly requested Class A default

Because the question explicitly assigns Class A, its historical default /8 supplies the intended network/host boundary. Keep first octet 10 and zero the remaining 24 host bits to obtain 10.0.0.0. If a different CIDR prefix were supplied it would override the default, but none is given in this class-specific question.

Why each choice is right or wrong

A - Correct: The Class A /8 default keeps first octet 10 and clears the remaining three octets.

B - Incorrect: This assumes a /16 boundary instead of the explicitly invoked Class A /8 default.

C - Incorrect: This assumes /24, retaining host bits that the Class A default would clear.

D - Incorrect: Clearing the network octet too loses the assigned Class A network identifier 10.

Primary note proof

Study-note section NET22

> Historical classes use leading patterns: A 0 with /8, B 10 with /16, C 110 with /24; D 1110 is multicast and E 1111 reserved. Ordinary class-A first octets are 1-126 because 0 and 127 have special uses. B spans 128-191 and C 192-223. Default usable counts are 2^24-2, 2^16-2 and 254. Modern CIDR requires the actual prefix and overrides class defaults.

Study-note section NET24

> Compute network=address AND mask. Host bits zero identify the block start; host bits one give broadcast. With 172.16.28.252/20, the third octet is grouped in blocks of 16, so the network is 172.16.16.0 and broadcast 172.16.31.255. A written host/prefix such as 172.105.180.0/21 need not be an aligned block label: masking yields 172.105.176.0/21.

Question sources

Data Communication & Networking review questions · Question 42

Question 267 | NS0614

UTP cable is most susceptible to which type of interference?

A. Thermal noise only

B. Electromagnetic interference (EMI) and crosstalk

C. Infrared interference

D. Gamma radiation

Hint

Apply the cited definitions to the stated scope; for calculations, derive the result from the supplied prefix, bit count or resource rule.

Answer B: EMI and crosstalk

UTP is unshielded copper: twisting reduces coupled interference but does not remove all electromagnetic coupling. NET06 identifies crosstalk as leakage from nearby channels. B names the relevant ordinary interference types, whereas thermal-only excludes other sources and infrared/gamma are not the note's cabling-susceptibility mechanism.

Why each choice is right or wrong

A - Incorrect: Thermal noise is not the only impairment; unshielded pairs can experience coupled electromagnetic interference.

B - Correct: EMI and adjacent-pair/channel crosstalk are relevant to unshielded copper, though twisting reduces coupling.

C - Incorrect: Infrared is an optical/unguided signaling category rather than the stated ordinary copper-coupling issue.

D - Incorrect: Gamma radiation is not the interference mechanism identified for UTP in the supplied note.

Primary note proof

Study-note section NET07

> Twisted pairs reduce coupled interference; UTP has no added shield and STP adds shielding. Coax has an inner conductor and outer shield sharing an axis. Fiber guides light and resists electromagnetic interference; it supports high capacity and long reach, but requires suitable optics and installation. Exact speed, cost and reach depend on the specification, not the material alone. Fiber can still be tapped.

Study-note section NET06

> Attenuation reduces signal strength. Distortion changes shape, often because frequencies have different delays. Noise adds unwanted energy: thermal noise comes from random thermal motion, crosstalk leaks from nearby channels, and impulse noise is a short disturbance. Amplifiers amplify noise too; digital repeaters regenerate decisions but cannot reconstruct every corrupted bit.

Question sources

Data Communication & Networking review questions · Question 43

Question 268 | NS0615

For a known unicast whose destination is on a different learned switch port in the same VLAN, what is the main forwarding difference between an active hub and an ordinary Ethernet switch?

A. Hubs operate at Layer 3; switches operate at Layer 2

B. Hubs send data to all connected devices; switches send data only to the intended device

C. Hubs use IP addresses; switches use MAC addresses

D. Hubs support fiber-optic; switches do not

Hint

Apply the cited definitions to the stated scope; for calculations, derive the result from the supplied prefix, bit count or resource rule.

Answer B: Hubs send data to all connected devices; switches send data only to the intended device

An active hub repeats incoming signals onto its other ports without examining addresses. A switch learns MAC-to-port mappings and, for the specified known unicast on another port, forwards the frame only to that destination port. Unknown unicasts and broadcasts are different cases and can be flooded. The scope restriction makes the intended contrast accurate without treating selective forwarding as a universal rule for all switch traffic.

Why each choice is right or wrong

A - Incorrect: Hubs are layer-1 repeaters, not layer-3 routers; ordinary switches are layer 2.

B - Correct: In this known-unicast case the hub repeats to other ports, while the switch sends only to the learned destination port.

C - Incorrect: Hubs do not use IP addresses to decide forwarding; they repeat signals without address inspection.

D - Incorrect: Hub versus switch is a signal-repetition versus frame-forwarding distinction; it does not impose the claimed prohibition on optical switch links.

Primary note proof

Study-note section NET10

> A bridge or ordinary Ethernet switch operates at layer 2. It learns source-MAC-to-port mappings, looks up the destination, forwards a known unicast to its port, filters it if the destination is on the incoming segment, and floods an unknown unicast or broadcast within its VLAN. A switch does not always send only to one destination port. Wireless access points normally bridge wireless and wired link-layer traffic.

Study-note section NET09

A repeater regenerates layer-1 signals without inspecting destination addresses. An active hub is a multiport repeater: it repeats incoming signals onto other ports, placing half-duplex endpoints in one collision domain. A passive hub is a connector. A hub neither learns MAC addresses nor eliminates collisions. An endpoint such as a network printer consumes services; routers, hubs and access points are intermediary devices.

Study-note section NET-S07

Ethernet switches can have fiber-optic interfaces with suitable optical transceivers. A forwarding role therefore does not impose a copper-only restriction: distinguish what the device does with frames from the physical medium used by its ports.

Question sources

Data Communication & Networking review questions · Question 44

Question 269 | NS0616

In multicast routing, data is sent to:

A. All devices on the network regardless of interest

B. A single specific destination

C. The nearest host among multiple hosts sharing an address

D. Only the devices that have expressed interest in receiving the data

Hint

Apply the cited definitions to the stated scope; for calculations, derive the result from the supplied prefix, bit count or resource rule.

Answer D: A subscribed/interested receiver group

NET30 distinguishes multicast group delivery from unicast, broadcast and anycast. Receivers express membership/interest in a group, rather than every network device receiving by definition or only one nearest destination being selected. D matches that destination-set meaning. Delivery still depends on the deployed network's forwarding and membership mechanisms.

Why each choice is right or wrong

A - Incorrect: All devices regardless of interest describes broadcast scope rather than multicast group selection.

B - Incorrect: One specific destination is ordinary unicast rather than a receiver group.

C - Incorrect: One nearest shared-address member is anycast.

D - Correct: Multicast targets a subscribed group of receivers that expressed interest.

Primary note proof

Study-note section NET30

> Flooding sends copies on eligible outgoing links with duplicate/lifetime controls; random walk picks a neighbor probabilistically. Unicast targets one destination, broadcast all in a scope, multicast a subscribed group and anycast one member sharing an address, normally nearest under routing metrics. Multi-destination packets can list multiple targets; this is not necessarily identical to broadcast. Group multicast trees use mechanisms such as reverse-path checks; Ethernet spanning tree is a different layer-2 mechanism.

Question sources

Data Communication & Networking review questions · Question 45

Question 270 | NS0617

What IPv4 address class is designed for multicast addressing?

A. Class A

B. Class B

C. Class C

D. Class D

Hint

Apply the cited definitions to the stated scope; for calculations, derive the result from the supplied prefix, bit count or resource rule.

Answer D: Class D

Historical IPv4 Class D begins with bits 1110 and is designated for multicast. Classes A, B and C describe historical unicast network allocations, with differing default prefixes. The question explicitly asks that historical class designation, so D is supported independently of how modern unicast prefixes are allocated.

Why each choice is right or wrong

A - Incorrect: Class A is historical unicast network space rather than the multicast class.

B - Incorrect: Class B is historical unicast space with a /16 default, not multicast.

C - Incorrect: Class C is historical unicast space with a /24 default.

D - Correct: Class D, identified by leading 1110, is designated for IPv4 multicast.

Primary note proof

Study-note section NET22

> Historical classes use leading patterns: A 0 with /8, B 10 with /16, C 110 with /24; D 1110 is multicast and E 1111 reserved. Ordinary class-A first octets are 1-126 because 0 and 127 have special uses. B spans 128-191 and C 192-223. Default usable counts are 2^24-2, 2^16-2 and 254. Modern CIDR requires the actual prefix and overrides class defaults.

Question sources

Data Communication & Networking review questions · Question 46

Question 271 | NS0618

Which OSI layer provides sequencing, acknowledgments and receiver flow control for end-to-end reliable process delivery, as in TCP?

A. Network Layer

B. Data Link Layer

C. Transport Layer

D. Session Layer

Hint

Apply the cited definitions to the stated scope; for calculations, derive the result from the supplied prefix, bit count or resource rule.

Answer C: Transport Layer

TCP uses sequence numbers, acknowledgments and windows to provide reliable ordered delivery between transport endpoints. Reliable link protocols can use similar mechanisms, but their scope is a single hop. The explicit end-to-end process requirement therefore selects transport. IP supplies best-effort network delivery, while session coordinates dialogs and checkpoints rather than defining TCP's ordered-byte-stream reliability and receiver flow control.

Why each choice is right or wrong

A - Incorrect: IP is best effort and does not supply the listed reliable acknowledgment/retransmission service.

B - Incorrect: Data-link reliability is hop-local rather than the required end-to-end process service.

C - Correct: Transport supplies TCP's end-to-end sequencing, acknowledgments and receiver flow control.

D - Incorrect: Session manages dialogs/checkpoints rather than the specifically listed link/TCP reliability machinery.

Primary note proof

Study-note section NET17

> TCP offers a reliable ordered byte stream using sequence numbers, acknowledgments, retransmission and windows. Flow control protects the receiver; congestion control protects network capacity. UDP sends independent datagrams with ports and a checksum but no built-in setup, delivery guarantee, retransmission or ordering. Live interactive traffic may choose UDP when late data is less useful than lost data. Application protocols can add reliability over UDP.

Study-note section NET14

> Controlled access uses polling, reservations or a token to grant turns; correctly coordinated access avoids contention collisions. Channelization divides frequency, time or code resources. Stop-and-wait sends one frame and waits for ACK, retransmitting on timeout; sequence bits distinguish duplicates. Sliding windows permit multiple unacknowledged frames. Link reliability/flow control is hop-local; transport reliability/flow control is end-to-end. Ethernet detects corruption but does not itself guarantee reliable delivery.

Study-note section NET19

> OSI session roles establish/manage dialogs and can coordinate checkpoints so transfer resumes after interruption. Presentation roles translate encodings and handle compression/encryption. Compression reduces representation size; encryption hides content and need not shrink it. Application protocols provide services directly to applications. Practical implementations

distribute these functions differently; TLS is not proof of a separate physical presentation-layer device.

Question sources

Data Communication & Networking review questions · Question 47

Question 272 | NS0619

For the IP address 192.168.2.64/26, what is the broadcast address?

A. 192.168.2.65

B. 192.168.2.126

C. 192.168.2.127

D. 192.168.2.255

Hint

Apply the cited definitions to the stated scope; for calculations, derive the result from the supplied prefix, bit count or resource rule.

Answer C: 192.168.2.127

A /26 has blocks of 64 addresses. Starting at .64, this block runs through .127; the final address has all six host bits one and is broadcast. .65 and .126 are ordinary first/last hosts. .255 belongs to another /26 block, so it is not this subnet's broadcast.

Why each choice is right or wrong

A - Incorrect: 192.168.2.65 is the first usable host, not the all-host-bits-one address.

B - Incorrect: 192.168.2.126 is the last usable host, one address below broadcast.

C - Correct: The .64-.127 /26 block ends at .127, its directed broadcast.

D - Incorrect: The .255 address is outside this .64-.127 subnet block.

Primary note proof

Study-note section NET25

> 192.168.2.64/26 spans .64-.127; usable .65-.126 gives 62 hosts. 192.168.10.25/28 spans .16-.31, so its network is .16. 172.17.128.0/21 spans 172.17.128.0-172.17.135.255; .128.255 and .135.0 are valid interior hosts, but .135.255 is broadcast. /27 gives 32 total and 30 usable, not 32 usable.

Study-note section NET24

> Compute network=address AND mask. Host bits zero identify the block start; host bits one give broadcast. With 172.16.28.252/20, the third octet is grouped in blocks of 16, so the network is 172.16.16.0 and broadcast 172.16.31.255. A written host/prefix such as 172.105.180.0/21 need not be an aligned block label: masking yields 172.105.176.0/21.

Question sources

Data Communication & Networking review questions · Question 48

Question 273 | NS0620

Which of the following CORRECTLY describes the role of SMTP?

A. Translates domain names to IP addresses

B. Governs how web pages are requested and delivered

C. Governs how email messages are sent from a client to a mail server

D. Enables file transfer between devices over the internet

Hint

Apply the cited definitions to the stated scope; for calculations, derive the result from the supplied prefix, bit count or resource rule.

Answer C: SMTP submits and relays email

NET21 assigns SMTP mail submission and relay. A client sending a message to a mail server is therefore a correct SMTP role. DNS resolves names, HTTP serves web requests and FTP transfers files. This does not assign end-user mailbox retrieval to SMTP; POP3/IMAP serve that separate task.

Why each choice is right or wrong

A - Incorrect: DNS resolves domain names to address records rather than SMTP.

B - Incorrect: HTTP governs web requests/responses, not SMTP.

C - Correct: SMTP submits mail from a client to a server and relays messages between mail servers.

D - Incorrect: File transfer is the FTP service role in this comparison, not SMTP's defining mail role.

Primary note proof

Study-note section NET21

> HTTP defines web request/response semantics; it is stateless, and a message body may be absent. HTTPS adds TLS protection. FTP transfers files using control and separate data connections; it is not the same protocol as SFTP. SMTP submits and relays mail; POP3 retrieves messages and IMAP accesses/synchronizes server mailboxes. Saying SMTP handles both sending and end-user mailbox retrieval is inaccurate.

Study-note section NET20

> DNS resolves names to records, including IPv4 A and IPv6 AAAA addresses; it can use UDP or TCP port 53. DHCP dynamically leases IPv4 settings, commonly address, mask, gateway and DNS server. Its basic exchange is discover, offer, request, acknowledge. IP itself does not assign addresses.

Question sources

Data Communication & Networking review questions · Question 49

Question 274 | NS0621

An omnidirectional antenna transmits signals in which pattern?

A. A narrow beam toward a specific target

B. Only vertically upward

C. In all directions simultaneously, creating 360-degree coverage

D. In a focused line-of-sight path only

Hint

Apply the cited definitions to the stated scope; for calculations, derive the result from the supplied prefix, bit count or resource rule.

Answer C: 360-degree azimuth coverage, with a nonuniform vertical pattern

NET07 defines omnidirectional as broad azimuth coverage. C is correct when its 360 degrees refers to the horizontal plane, not equal power in every three-dimensional direction. Directional beams or upward-only radiation do not describe this pattern. Antenna elevation patterns can still have lobes/nulls, so the answer retains that scope qualification.

Why each choice is right or wrong

A - Incorrect: A narrow targeted beam is directional rather than omnidirectional azimuth coverage.

B - Incorrect: Upward-only radiation does not provide the broad around-the-antenna azimuth pattern.

C - Correct: 360-degree azimuth coverage is the intended meaning, without asserting equal power in all three-dimensional directions.

D - Incorrect: A single focused path describes a directional antenna pattern.

Primary note proof

Study-note section NET07

> Radio, microwave and infrared are unguided media. Ground waves follow Earth, sky waves can reflect from ionized layers, and line-of-sight paths require suitable visibility. Microwaves are radio waves in the broader physical classification. Infrared generally does not penetrate walls. Directionality depends on antennas: omnidirectional means broad azimuth coverage, not equal radiation in every 3-D direction. Legacy Ethernet straight-through cables join unlike MDI/MDI-X roles; crossover joins like roles, such as PC-PC or switch-switch. Auto-MDI-X can remove that requirement.

Question sources

Data Communication & Networking review questions · Question 50